

Geographic Decentralization in Web3 Networks

Executive Summary

Geographic decentralization refers to the physical distribution of a network's critical components (nodes, validators, infrastructure) across diverse locations and jurisdictions. In blockchain and Web3 systems, strong geographic decentralization is argued to bolster censorship-resistance, fairness, and resilience against localized failures ¹ ². This report examines how “decentralization of power must be global” ³, exploring what that means at different layers (from individual nodes to legal jurisdictions) and how it might be quantified or incentivized. We find that measuring geographic decentralization is complex and often controversial: many experts caution against simplistic metrics that give a false sense of precision ⁴. Nonetheless, various approaches exist – from mapping node IP addresses to analyzing latency – each with strengths and pitfalls.

We survey **state-of-the-art techniques for inferring node locations**: direct node telemetry, IP geolocation, cloud provider fingerprinting, latency-based triangulation, BGP route analysis, active network probing, and more. Each method yields partial insight (e.g. identifying a node's country or hosting provider) but comes with accuracy limits and failure modes (like VPNs obscuring true location, or geolocation databases being imprecise). **A recurring theme is the risk of false precision – detailed-looking maps or statistics that may conceal large uncertainties** ⁴. The report highlights critiques from networking research and security literature that urge caution in interpreting such data.

Major blockchain protocols have taken varied stances on measuring and publicizing their geographic distribution. For example, Ethereum's researchers acknowledge a “heavy concentration along the Atlantic” (Europe and U.S. East Coast) among validators ⁵ and are studying how protocol design (e.g. block propagation methods) influences this clustering ⁶ ⁷. Bitcoin historically saw over half of its mining power concentrated in a single country (China) before a 2021 ban forced a global reshuffling ⁸. Networks like Solana and Polygon have noted their node distributions, with Polygon reporting that no single country hosts more than one-third of its validators ⁹ – yet also acknowledging reliance on a few cloud providers for over half of nodes ¹⁰. We review such metrics used (or avoided) by Ethereum, Bitcoin, Solana, Cosmos, Filecoin, Polygon, and Layer-2 networks, noting points of consensus and controversy. **Often, public communications celebrate global reach, while internal discussions focus on worrisome concentrations (such as too many validators in one region or on one cloud)**. Academic and industry analyses provide independent critiques – for instance, studies showing **a significant portion of Ethereum blocks in 2022 were filtered to comply with U.S. sanctions** ¹¹ ¹², raising questions about the network's geographic and political decentralization.

The report also draws from adjacent fields to enrich the discussion. **Lessons from telecommunication infrastructure and Internet topology mapping show how physical routes and choke points can create hidden centralization. Content delivery networks and internet exchange points illustrate the benefits and limits of geographic dispersion in reducing latency. We examine analogies in power grids and supply chains, where dependency on one region (for energy or components) is seen as a systemic risk – a parallel to having too many blockchain nodes in one jurisdiction or data center. Frameworks for systemic risk and disaster recovery planning highlight the value of decentralizing critical operations to survive regional outages. We identify which frameworks map well to blockchain networks (e.g. measuring jurisdictional diversity of nodes is akin to measuring supply-chain diversity ¹³ ¹⁴) and why others do not (e.g. governmental decentralization indexes don't translate neatly to open networks).**

We compare competing frameworks and taxonomies for decentralization. Some efforts focus purely on consensus or stake distribution, while others (including recent standards from industry) emphasize **operational decentralization** across geography, infrastructure, and software diversity^{13 14}. We discuss the popular **Nakamoto coefficient** (the minimum entities needed to compromise a system)¹⁵ and how it can be applied to geographic units (e.g. the smallest number of regions whose failure would halt a network¹⁶). We contrast this with metrics like the *geographic Gini/Herfindahl* indices (measuring inequality of stake distribution across regions)¹⁷ and more nuanced proposals (e.g. **Ethereum researchers' liveness coefficient** counting how many top regions must fail to threaten the chain¹⁶). While there is some consensus that decentralization is multi-dimensional, definitions diverge on which dimensions matter most. Notably, geography has often been under-represented in formal metrics – a gap now being actively addressed by new research^{18 5}.

Our analysis of **structural risks** finds that geographic concentration can undermine core promises of blockchain networks. Censorship resistance suffers if most validators fall under one jurisdiction's laws (as seen when >40% of Ethereum blocks post-Merge were OFAC-censored^{11 12}). Correlated failures become likely if nodes share infrastructure – for example, an outage at a single cloud provider (AWS US-East) in 2025 knocked out ~37% of Ethereum nodes^{19 20} and disrupted multiple “decentralized” services. Legal and regulatory actions can have outsized impact (e.g. a single country's ban on mining or staking causing a global shock⁸). Reliance on major cloud and hosting companies means **single points of failure** contrary to the decentralization ethos^{21 22}. We describe scenarios like national firewalls or power grid outages: if too much of a network is concentrated in one region, an event there (natural disaster, conflict, blackout) could impair the network's availability or performance. Case studies and modeling from both blockchain and traditional infrastructure domains underscore the need for **geo-diversity as a buffer** against these threats.

Crucially, we identify **gaps in the field**. Data on node locations is often incomplete – for instance, many nodes run behind NATs or use privacy networks, escaping detection^{23 24}. Current methodologies can break down: IP-based inference struggles with VPNs or IPv6, latency methods can be spoofed, and operator identities are not always public. There is also a lack of longitudinal data – few projects track how decentralization evolves over time, making it hard to backcast trends or detect early signs of re-centralization. We note the paucity of agreed-upon standards: each project or researcher may define and measure decentralization differently, complicating comparisons. These gaps point to a need for new techniques and collaborative efforts to better measure (and improve) geographic decentralization.

The report concludes by proposing a **hybrid measurement methodology** that combines the strongest elements of existing approaches. We suggest using multiple inference modalities in parallel – e.g. correlating IP geolocation with latency triangulation and cloud provider data – to cross-verify node locations. Transparent weighting should be applied: clearly explaining how each data source contributes to the final assessment (and giving more weight to high-confidence signals). The methodology must be reproducible, with open data and code, so that results can be audited and improved by the community. We emphasize providing uncertainty bounds for any reported metric (for example, giving a range for how many nodes are in a region with X% confidence, rather than a single number). All assumptions – such as trust thresholds for triangulation or coverage limitations of a scanner – should be explicitly documented. This hybrid approach cannot magically reveal everything (for instance, truly hidden or spoofed nodes will remain elusive), and it cannot **guarantee** a network is safe from centralization. However, it can paint **a more robust and honest picture of the geographic layout of a network, which is a starting point for mitigation**.

Finally, we outline a **roadmap for further research and action**. Key steps include gathering better data (e.g. encouraging nodes to opt-in to share anonymized location info), building cross-disciplinary collaborations (between blockchain devs and Internet measurement experts, geographers, etc.), and

pushing for community standards on decentralization metrics. We highlight the potential of new *proof-of-location* schemes (some using trusted hardware or coordinated delay measurements ²⁵) that could allow networks to verify node locations in a decentralized way – a promising area for technical experimentation. The roadmap also calls for **scenario drills and simulations (like “geo-disaster recovery” tests) to see how networks cope with regional outages**, informing where improvements are needed. By pursuing these steps, the Web3 community can move toward a more rigorous, data-driven understanding of decentralization and avoid the trap of mere rhetoric.

In sum, geographic decentralization in Web3 is multi-faceted and vital, but measuring and achieving it remain challenging. This report provides a comprehensive survey of the concepts, methods, current state, and future directions needed to ensure that decentralized networks truly span and withstand the world.

Annotated Outline

- **1. Clarifying the Object of Study:** Defines “geographic decentralization” across different layers – the network topology, node operators, physical infrastructure, and legal jurisdictions. We discuss how each layer offers a lens on decentralization (e.g. distribution of nodes on the network vs. distribution of control by entities vs. distribution across countries). This section also covers philosophical debates on measurability: whether decentralization can be quantified or is inherently qualitative. We highlight viewpoints that only *power* distribution matters ²⁶, as well as those cautioning against oversimplified metrics ⁴.
- **2. Survey of Existing Measurement Techniques:** An in-depth look at how researchers and practitioners currently assess geographic spread. For each major technique – node telemetry, operator mapping, IP-based geolocation, cloud provider fingerprinting, latency and triangulation, BGP route analysis, active probing, metadata extraction – we describe how it works and what aspect of location it captures. We enumerate accuracy limits (e.g. IP geolocation might locate a node only to a country or city, with a margin of error) and typical failure modes (such as nodes deliberately obscuring their location via Tor or VPN). We discuss sources of error (like outdated IP databases or clock skew affecting latency measures) and warn of “false precision” risks, drawing on networking literature that shows how easy-to-measure proxies can mislead ⁴. Where available, we include critiques from security researchers who have attacked or improved these techniques.
- **3. Decentralization in Major Protocols (Case Studies):** Examines how leading blockchain networks address geographic decentralization in theory and practice. We cover **Ethereum, Bitcoin, Solana, Cosmos, Filecoin**, and major Layer-2s (including **Polygon** as requested). For each, we note any metrics they publish or studies conducted on node distribution. For example, Ethereum’s community has public dashboards of node locations (Ethernodes, etc.) and internal research quantifying its Atlantic-heavy validator clustering ⁵. Bitcoin’s case includes mining geography shifts (e.g. the China ban and subsequent U.S. rise ⁸) and known node distribution from surveys. We present what these projects emphasize publicly (often broad global reach) versus concerns raised internally or by outsiders (such as reliance on data centers or specific countries). We also cite any critical papers or reports – e.g. studies highlighting Solana’s dependency on a few hosting providers, or analyses of Cosmos chains’ validator sets. Points of controversy (like debates over how much decentralization is “enough” or whether certain networks are decentralized at all) are noted.

- **4. Insights from Adjacent Fields:** Brings perspectives from outside pure blockchain. We discuss **telecommunications resilience** (how diversified telecom infrastructure prevents single points of failure and what blockchain networks can learn from it). We look at **Internet topology research** – for instance, the importance of multiple backbone routes and the role of IXPs (Internet Exchange Points) – drawing parallels to peer-to-peer networks. **Content Delivery Networks (CDNs)** and their geographic caching strategies inform how latency and location impact performance. We connect to **energy grid redundancy**, noting that just as an electrical grid benefits from distributed generation to avoid blackouts, blockchains benefit from nodes on independent power sources. **Supply chain concentration metrics** (like Herfindahl indices for supplier diversity) are analogous to measuring how distributed validators are across providers or regions ¹³. **Systemic risk modeling** in finance (which gauges how a shock in one node of a network cascades) helps model blockchain failure scenarios. **Disaster recovery planning** (as done in critical industries) offers frameworks for ensuring continuity despite losing a region. We identify which analogies hold strongly – for example, jurisdictional decentralization is much like diversifying suppliers to reduce collective risk – and which don’t – for example, government decentralization indices don’t account for physical network effects.
- **5. Comparing Frameworks and Taxonomies:** Reviews various formal attempts to define and measure decentralization. This includes **academic proposals** (like metrics in peer-reviewed papers), **industry frameworks** (e.g. ConsenSys’s multi-metric approach ²⁷ or Messari’s operational decentralization criteria ¹³ ¹⁴), and any **standards-body discussions** (if organizations like the IEEE, ISO, or others have weighed in). We detail what each framework measures – for instance, some focus on consensus (stake or hash power distribution), others on network topology, others on governance. We highlight what they miss – e.g. many don’t explicitly measure geography or assume it indirectly. Areas of consensus (such as broad agreement that no single metric suffices) and divergence (such as differing definitions of “decentralized enough”) are explained. We pay special attention to how each framework treats geography: some implicitly assume it via independent failure domains, while others (like recent Ethereum research ¹⁸) explicitly incorporate it. This section also introduces concepts like the **Nakamoto coefficient** ¹⁵ and newer ideas (e.g. “cost of corruption/kidnapping” metrics that consider the real-world effort to compromise nodes in various locations).
- **6. Structural Risks of Geographic Concentration:** Analyzes why geographic clustering can be dangerous for a supposedly decentralized network. We break down several impact areas:
 - **Censorship Resistance:** When many nodes are under one government’s jurisdiction, that authority can enforce transaction censorship or block certain participants (we cite the Ethereum OFAC censorship episode as a real example ¹¹ ¹²).
 - **Correlated Infrastructure Failures:** Nodes co-located in one area might all be affected by the same power outage, natural disaster, or ISP failure. We give instances like cloud outages taking out large chunks of nodes (e.g. AWS issues affecting 37% of Ethereum nodes ¹⁹) or country-wide internet shutdowns that could partition a network.
 - **Legal and Regulatory Intervention:** A single country hosting a majority of a network can effectively impose regulations on it (for example, the U.S. or EU could claim authority since so many validators reside there). We mention scenarios like mining bans (China 2021 ⁸) or new laws that force node operators to comply with local rules, undermining global neutrality ²⁸ ²⁹.
 - **Cloud/ISP Centralization:** Reliance on a few big cloud providers concentrates risk – those companies might have failures or might decide unilaterally to ban certain blockchain activities. We discuss how **Hetzner and AWS** have been flagged for hosting outsized portions of Ethereum, Solana, etc., and what happens if they disconnect service (pointing to the “if AWS is down and your blockchain stops, it’s not decentralized” argument ³⁰).

- **National-Scale Outages:** We explore thought experiments and past events – e.g., if **Kazakhstan** (a major Bitcoin mining hub post-China) had an internet blackout (as occurred briefly during unrest) or if **Europe** experienced a coordinated power grid issue, how would those events ripple through Bitcoin or Ethereum? The analysis uses models of node distribution to gauge at what point liveness or consensus might break ¹⁶.
- **Operational Capacity in Crises:** In a global crisis (pandemic, war, extreme climate event), networks with geographically concentrated personnel might struggle to maintain operations (node maintenance, upgrades, etc.). We relate this to disaster recovery principles – networks should have enough spread that some part can always pick up slack.

Throughout this section, we incorporate scenario modeling and comparative cases from literature (for example, studies that simulate removal of entire regions from the network ³¹ ³²). The goal is to show concretely how geography translates to systemic risk.

- **7. Gaps and Challenges in the Field:** Highlights what's missing in our current understanding and toolkit. We note the **data gaps** – for many networks, we lack reliable data on node location over time, especially for those that do not publish it or where nodes hide behind privacy tools. **Methodological limitations** are listed: for instance, scanning the peer-to-peer network finds only *reachable* nodes, omitting perhaps half the nodes that are firewalled or use private connections ²³ ²⁴. Inference methods can conflict (IP vs latency might give different results), and validating which is correct is hard without ground truth. We also point out **new centralization vectors** that aren't well captured: e.g., the growth of professional staking services that might distribute nodes globally but constitute a single operator (power centralization not obvious from geographic data alone). Additionally, we address where **methodologies break** – for example, if adversaries intentionally misreport or obfuscate location, most current measures cannot detect that. The section calls attention to the risk of focusing on easily measurable aspects (node count, etc.) while ignoring harder-to-measure ones like social or governance centralization (who controls those nodes). We conclude that without better data and refined methods, any decentralization index will have significant blind spots.

- **8. Toward a Hybrid Measurement Methodology:** Proposes a way to combine multiple approaches for a more reliable assessment. We suggest integrating:

- **Multi-modal data collection:** Use a combination of peer-to-peer crawling (to get IP addresses), active latency probing (to estimate distances), cloud provider APIs (to identify hosting services), and perhaps voluntary self-reported metadata. Each modality can catch something the others miss.
- **Cross-verification and weighting:** For each node, cross-check location indicators (does the IP's reported country match latency clues? Is the ASN (autonomous system) belonging to a known cloud region?). Define a scoring system that weighs these clues based on confidence. For example, a node might be 90% likely in Germany if multiple indicators align, but only 50% confident if clues conflict.
- **Transparent and reproducible logic:** We advocate open-sourcing the methodology – e.g. publishing the code or Datasets – so others can reproduce the results or adjust parameters. This builds trust and allows collective improvement. Any filtering (like discarding outlier data) should be documented.
- **Uncertainty quantification:** Rather than stating “X% of nodes are in country Y” with absolute certainty, present ranges or confidence intervals. For instance, “We estimate 25–30% of nodes in the U.S., with uncertainty due to 10% of nodes that could not be geolocated precisely.” This acknowledges measurement error.

- **Explicit assumptions:** Clearly list assumptions such as “IP address roughly correlates to physical location except where proxies are used” or “at least 80% of nodes respond to our probes”. If the method assumes an honest subset of nodes for triangulation (as some proof-of-location protocols do ²⁵), state that and consider the impact if the assumption fails.

We illustrate this hybrid method with a hypothetical example (or an existing pilot study if any exist), and we clarify the method’s **scope**: **it can map and monitor decentralization to an extent, but it cannot guarantee security or decentralization**. For instance, even a widely spread network could be vulnerable if a single actor owns many of those nodes (power vs geography discrepancy). The hybrid approach can highlight such discrepancies if combined with on-chain data (stake ownership) – another integration we propose. In summary, this section sketches a blueprint for a more trustworthy “decentralization index” that could be iteratively refined.

- **9. Roadmap for Further Research and Action:** Outlines future steps to advance both measurement and actual decentralization. We identify potential **data sources** to tap into: for example, collaboration with projects like ProbeLab (which monitors Ethereum’s DHT network health) to access their ongoing data ³³ ³⁴, or engaging with cloud providers to share aggregate stats on nodes (if privacy can be preserved). We propose **collaborations** between academia, industry, and maybe even regulators, to define standard metrics – similar to how the Internet community has RFCs for uptime or routing statistics. A **standards effort** could be initiated through bodies like the Ethereum Foundation, W3C, or ITU to agree on decentralization benchmarks (for instance, a standard way to calculate a “geographic diversity score”). We also suggest technical experiments: e.g. deploying measurement nodes around the world (a “planetary network telescope”) to continuously triangulate blockchain nodes – building on ideas from research like BFT-PoLoc which uses distributed vantage points to prove location ²⁵. Another idea is **incentivized testnets** where node operators are rewarded for providing verifiable location info (perhaps via protocols that use GPS or timing proofs), to see how behavior changes. We call for more **historical analyses** – using whatever data is available to plot how distribution changed from, say, 2015 to 2025 for major networks, which could reveal centralization trends early. Finally, we emphasize outreach: educating the community that decentralization has many axes and that running nodes in diverse places matters. The roadmap suggests that improvements in decentralization will likely come from a mix of protocol design changes (to reduce the advantage of being in one spot) and off-chain efforts (diversifying infrastructure, encouraging hobbyist nodes globally, etc.).

- **10. Embracing Methodological Transparency:** Stresses the importance of honesty and clarity in any research or claims about decentralization. In this concluding section, we reflect on the need to **clearly distinguish facts from inferences** in our own analysis and any future reporting. For every statistic presented, the reader should know whether it’s directly measured (e.g. “30% of nodes responded from IPs in Germany” is a direct observation) versus derived (e.g. “therefore 30% of stake is in Europe” might be an assumption if stake-to-node mapping isn’t exact). We champion Angela Walch’s warning against letting convenient metrics “crowd out” more meaningful assessment ⁴. Thus, we propose that **any decentralization index or report should come with a methodological appendix that itemizes data sources, assumptions, potential error margins, and areas of uncertainty**. In practice, maintaining this transparency builds credibility and allows domain experts (like network engineers or statisticians) to input on specific uncertainties. We also acknowledge the dynamic nature of the field – what is uncertain today (e.g. exact node counts in cloud environments) might be resolved tomorrow with new data, so transparency helps track the evolution of knowledge. This section serves as a reminder that decentralization is not just a number to maximize, but a complex state that we must continually probe with humility.

With this outline guiding the detailed content, the report now delves into each section in turn, providing a thorough exploration of geographic decentralization in Web3 networks.

1. Clarifying the Object of Study

Defining “Geographic Decentralization” at Different Layers: At its core, geographic decentralization describes how spread out a network’s critical participants and infrastructure are across physical space and political boundaries. We can distinguish several layers or aspects:

- **Network Layer (Physical Topology):** This refers to where the nodes (servers running the protocol) are located on the globe and how they connect. A *geographically decentralized network* at this layer means nodes are widespread across cities, countries, and continents, rather than clustered in one region. For example, if nodes are evenly dispersed worldwide, no single outage or local event can take them all down. In contrast, if most nodes sit in one data center or one country, the network is geographically centralized in that physical sense. Researchers increasingly recognize that decentralization “has a geographic dimension that conventional metrics such as stake distribution overlook”³⁵ – meaning even if ownership is decentralized, if all machines are in one place, the system is vulnerable.
- **Operator/Ownership Layer:** This considers *who runs the nodes* and where those entities are based. One can imagine a scenario where nodes are scattered in different countries, but all owned by a handful of companies located in the same jurisdiction – that would be decentralized physically but centralized in governance. Conversely, if many independent operators each run nodes in various locations, power is more diffuse. The Polygon team suggests evaluating decentralization by the “total distinct entities running the validator nodes” and their distribution³⁶. We extend this: geographic decentralization at the operator layer asks whether those entities are themselves spread globally (e.g. a mix of operators from different countries) or concentrated (e.g. all major mining firms headquartered in one country).
- **Infrastructure Layer:** This focuses on the underlying infrastructure providers and hardware. Even if nodes are nominally run by different people, if they all rely on the same *cloud service or internet provider*, the system isn’t truly independent. A geographically decentralized infrastructure means nodes use *diverse data centers, ISPs, power grids*, etc. For instance, a network where half the nodes run on Amazon Web Services in one region is less decentralized infrastructure-wise than one where nodes run on a mix of AWS, Google Cloud, Hetzner, home servers, and so on around the world. Polygon’s report explicitly measures “distribution of cloud providers running the validator nodes” as a decentralization factor³⁶. Geographic decentralization at this layer often overlaps with the network layer (since clouds are in specific regions), but it adds the aspect of corporate diversity – a form of *vendor decentralization*.
- **Jurisdictional/Legal Layer:** This layer is about *political geography* – the countries or legal jurisdictions that nodes and operators fall under. A network spread across many jurisdictions is harder for any single government to unilaterally control or shut down. For example, if nodes are in 100 different countries, no single national law can directly affect more than a fraction of the network. In contrast, if 80% of nodes are in one country, that country’s regulations (or sanctions) could effectively apply to the network’s majority. The jurisdictional layer is subtly different from physical location: for instance, an island hosting a data center may physically concentrate nodes, but if it’s an independent nation with different laws than, say, the U.S. or China, it still adds *regulatory diversity*. Polygon notes that in their network, while most nodes are in North America or Europe, “the distribution across different legal jurisdictions is quite broad” – with no single country over one-third⁹. This highlights looking beyond continents to legal boundaries.

These layers interrelate. We often desire decentralization *across all of them*: e.g. many independent operators, running on diverse infrastructure, located in many countries. However, these aspects can also diverge. For example, one could have geographic decentralization at the network layer (nodes all over) but not at the operator layer (if one entity owns those globally scattered nodes). Thus, part of

clarifying the object is understanding that “decentralization” is not a monolith – a theme echoed by many experts ³⁷ ³⁸ .

Philosophical and Methodological Debates: Is geographic decentralization actually measurable? Opinions vary: - Some argue that **power distribution is the only “real” decentralization, and geography is only relevant insofar as it influences power**. Phil Daian encapsulates this view: “The only decentralization that matters is decentralization of power” ²⁶ . In this view, if power (control over block production, consensus, etc.) is decentralized among many actors, then the system is decentralized – and those actors will *likely* be geographically diverse as a consequence. Therefore, one might deprioritize direct geographic metrics, focusing on who has influence. However, Phil also notes that **power must be global** – suggesting that if all power-holders are in one region, it contradicts the goals of neutrality and permissionlessness ³ . So even this perspective loops back to geography, but indirectly (power must not be geographically concentrated). - Others believe that **geographic decentralization is an inherent good** in decentralized systems, underpinning properties like neutrality, fairness, and robustness. The Flashbots team and others argue that a system biased towards one region cannot truly claim neutrality or fairness ³⁹ ⁴⁰ . Under this philosophy, *where* validators or miners are matters a great deal – and should be measured and maximized. The debate arises on how to measure “where.” Is it by count of nodes per country? By share of stake per region? By something like latency influence (as Phil’s definition based on latency sensitivity proposes ⁴¹)? - A big methodological debate is **quantitative vs qualitative**. Traditionalists might say decentralization is a fuzzy, multidimensional concept that resists being boiled down to numbers. In contrast, many in the blockchain space attempt to attach metrics (node counts, Nakamoto coefficients, Gini coefficients of distribution, etc.) to it. Angela Walch, a legal scholar, critiques the community’s loose use of “decentralization” and warns of “**Gresham’s Law of Measurement**” – the idea that easy-to-measure metrics could overshadow more meaningful but harder-to-measure aspects ³⁸ . For example, counting nodes is easy, but does it really reflect decentralization if many nodes are semantically redundant or controlled by the same entity? Walch suggests that chasing a single quantitative score might give the illusion of objectivity while missing the essence ⁴ . This debate implies we must be careful: yes, we should measure what we can, but we must acknowledge what we can’t (or what the measurements proxy for). - Another debate: **Static vs Dynamic measurement**. Some researchers argue that even if you measure geographic spread now, what matters is how the network *evolves*. A network could be decentralized today but centralizing over time due to economic forces (e.g. validators clustering to reduce latency costs ⁷ ⁴²). There’s discussion on whether we need metrics that capture *tendencies* or *incentives* to centralize, not just snapshots. For instance, Vitalik Buterin and others have mused about decentralization as an *emergent property* that can change with context (like when hardware requirements grow, fewer people can participate, reducing geographic spread). This connects to whether it’s measurable: you might measure current geography but not capture latent risks. Some proposals (like Phil Daian’s definition using x vs x' profit for low-latency players ⁴¹) try to formalize whether a protocol inherently pushes nodes to cluster.

Whether geographic decentralization is measurable at all is also a practical question: nodes can be pseudonymous. On many networks, there’s no built-in reporting of location. So any measurement is indirect. Some critics say any numbers you see (like “X% of nodes in country Y”) are inherently rough estimates, not ground truth – because truly, no one knows where all the participants are if they don’t want to be known. This skepticism doesn’t mean we shouldn’t try to measure, but we should do so knowing the limitations.

In summary, the object of study – geographic decentralization – can be thought of as a vector with multiple components (technical, operational, jurisdictional). It’s important *why* we care: a key assumption is that geographic decentralization contributes to a network’s goals of **permissionlessness, fairness, global applicability, and resilience** ⁴³ ² . If we couldn’t reason that geography affects

these, measuring it would be less meaningful. But evidence (and intuition) shows it does: co-location can give undue advantage or create single points of failure ⁴² ¹. Hence, even if tricky, we attempt to measure it. We proceed with a clear understanding that any metric is a proxy, and we must interpret it in context, keeping transparency (as emphasized in Section 10) about what is *measured*, what is *inferred*, and what remains *uncertain*.

2. Survey of Existing Measurement Techniques

Measuring the geographic distribution of nodes in a Web3 network is inherently challenging – there’s no GPS built into Bitcoin or Ethereum nodes advertising their coordinates. Instead, researchers rely on a variety of techniques, each with its own scope and pitfalls. Here we survey major categories of measurement and their characteristics:

Node-Level Telemetry and Self-Reporting

Technique: Some blockchain clients or community tools allow nodes to report certain telemetry data, which could include location hints. For example, a node might voluntarily tag itself (in metadata or node description) with a location or might participate in a monitoring network that logs latency to other nodes (which can indicate distance). In Ethereum’s case, there isn’t a standard self-reported location field, but there are community efforts like Ethstats or Node Explorer sites where node operators can register and show location on a map. Another form of telemetry is simply the node’s IP address and port – which every reachable node discloses as part of peer-to-peer networking. While an IP isn’t an explicit “I am in London” statement, it’s a key input for other methods (geolocation, etc.).

What it Measures: If explicit, telemetry can directly measure a node’s stated region (though this is rare and not trustless). Implicitly, by gathering raw data from nodes (like IP, latency to a few well-known servers, etc.), it provides the raw material to infer location. Node-level telemetry could also measure things like which other nodes it’s connected to (giving hints of network topology and possibly physical proximity if clusters form).

Accuracy Limits: Self-reported data can be **very accurate** if honest (the operator knows where they are), but there’s no guarantee of honesty or consistency. An operator might mislabel location for privacy or fun. Relying on voluntary reporting typically gives a partial view (only those willing to share). In terms of IP collection (a form of telemetry since nodes share addresses in P2P protocols), not all nodes are reachable – many operate behind NAT or proxies, meaning the IP seen might be of a gateway or just not obtainable at all ²³. So telemetry might capture only a subset (e.g. ProbeLab notes their Ethereum crawl “only able to display information about dialable nodes” ²³, missing those behind NAT). This can skew results if, say, home users (possibly more geographically dispersed) are underrepresented because they’re behind NAT, while data center nodes (often have public IPs) are overrepresented.

Typical Failure Modes: A big issue is **selection bias** – the nodes you can monitor or that opt in are not random. For instance, if mostly hobbyists in the U.S. sign up for a node map, the map will show a U.S.-heavy network even if actual distribution is different. Another failure mode is **inaccuracy of reported data** – someone might accidentally or intentionally provide wrong info (saying “Antarctica” as a joke). Telemetry might also fail as nodes churn; a snapshot could be outdated quickly as nodes go offline or move.

Sources of Error: Clock skew or timing issues can corrupt telemetry (if measuring latency, a node’s slow clock might mis-estimate distances). If using node IDs or metadata, one might mistakenly treat multiple nodes run by one person as separate data points in distribution, thus over-counting (though this is

more about operator mapping). If relying on IP from node messages, errors include the node giving a placeholder IP (some protocols allow advertising 0.0.0.0 or private IPs which are non-geographic).

False Precision Risks: Presenting telemetry results without caveats might suggest “we have 100% accurate map of nodes,” which is rarely true. For instance, Ethernodes (which uses a crawler akin to telemetry) lists nodes by country with percentages to two decimal places. Those numbers can imply a precision that belies the fact that some nodes couldn’t be located at all and others might be mis-located. Researchers caution that such metrics should ideally include confidence intervals or at least note the unseen portion ⁴⁴.

Use in Literature: A notable use of peer-to-peer telemetry was by Kim et al. (2018), who crawled Ethereum’s network and inferred locations of nodes; they found in 2018 that **43.2% of Ethereum’s nodes were in the U.S., 12.9% in China, 5.2% in Germany** ⁴⁴. This was done via collecting node IPs from the network (a telemetry approach) and mapping them. This kind of study shows both the power (it yielded concrete numbers) and the dated nature (those numbers were PoW-era Ethereum; things have changed, and indeed later crawls in PoS era still show “continued concentration in a few countries” ⁴⁴). It’s a baseline but must be updated continuously to remain useful.

Operator-Level Mapping and Entity Attribution

Technique: Rather than focusing on individual nodes as points, this approach groups nodes by their operator or controlling entity, and sometimes by that entity’s location. It often involves detective work: identifying which nodes belong to the same mining pool, staking provider, company, or individual. Techniques include analyzing on-chain data (e.g. which validators have the same payout address or are known affiliates) and off-chain info (announcements like “Exchange X runs Y validators in region Z”). For example, in proof-of-stake networks, one might group all validators operated by a service like Binance or Coinbase, and then note that those companies are headquartered in specific countries (U.S., etc.). In Bitcoin’s mining context, *hashrate attribution* to pools is common ⁴⁵, and pools often have known base countries (though miners within a pool are globally distributed, which complicates using pool HQ as a “location”).

What it Measures: This maps *power structure* over geography. It can measure the decentralization of governance or control in geographic terms. For instance, if we find that 60% of validators are run by five entities and all five are in the same country, that’s a key insight (even if the nodes themselves might be spread out physically, the decision-making and legal liability concentrate). Operator mapping can also measure diversity of jurisdictions of entity headquarters, which is slightly different than node locations but very relevant for legal risk.

Accuracy Limits: Identifying operators can be tricky and sometimes speculative. Some networks have *registries* (e.g. EOS had a list of block producers, many of which were entities that could be looked up for location). Others like Ethereum do not – but researchers have de-anonymized validators by pairing consensus-level identifiers with networking data ⁴⁶. Heimbach et al. (2025) managed to *deanonymize Ethereum validators via the p2p network* ⁴⁶, essentially linking validators to IPs and thus to geography and possibly to known hosting providers. That is a cutting-edge example showing it’s possible to get operator info, but it required sophisticated analysis. The accuracy can be high for known pools or companies (you can be quite sure who Coinbase is and that it’s U.S.-based), but much lower for independent or pseudonymous operators (an individual running a node at home – we might only know their IP or nothing at all).

Typical Failure Modes: A big challenge is **shared infrastructure**: If multiple operators use the same cloud or staking-as-a-service platform, mapping by entity might mistakenly lump them or miss that they

share a failure point. Conversely, an operator might run nodes in multiple countries; mapping by operator might oversimplify to one location. Another failure is that some entities are decentralized themselves (e.g. DAO-operated nodes with members globally), making it hard to assign a single geography. And there's the risk of **misidentification** – false positives/negatives in grouping. For instance, two node IDs might appear related but are actually different people in the same region (false grouping), or vice versa.

Sources of Error: On-chain data can mislead – e.g. if two validators use the same withdrawal address, one might assume one operator, but maybe it's a coincidence or a shared custody service. IP-based grouping might group nodes on the same subnet as one operator, but that could be an ISP CGNAT grouping unrelated users. Often, heuristics are used, which can carry error (like grouping by very close node enode IDs or gossip network patterns might not always reflect single operator).

False Precision Risks: Claiming “there are N distinct operators” with a precise number can be risky if the identification isn't certain. Also, stating “Operator X in country Y controls Z%” might ignore that operator's nodes are worldwide – thus potentially underestimating geographic spread. Conversely, it might give a sense of security (“we have 50 independent operators”) without noting many might all be in one locale or dependent on one supplier (a nuance lost if focusing solely on count).

Use in Literature: The concept of the **Nakamoto coefficient** is an operator-level (or at least entity-level) measure: it asks how many entities to compromise to control the system ¹⁵. Geographic versions exist implicitly: e.g., the liveness Nakamoto coefficient by region ¹⁶ counts how many top regions (by stake) would need to fail. That is akin to treating each region as an “operator” for failure. The Messari 2023 report explicitly calls for examining stake distribution across both infrastructure and geographic jurisdictions ¹³, combining operator concentration with geography. Cambridge's CCAF analysis, while mostly focusing on node count, also implicitly acknowledges operator concentration by highlighting that many nodes are hosted (meaning possibly few hosting companies) ¹⁹. So, while operator mapping is sometimes separate (focusing on control, not physical location), when you tie an operator to a country, you bridge to geographic decentralization – e.g., knowing 4 of the top 5 Ethereum staking entities are based in the U.S. tells you a lot about potential jurisdictional concentration.

IP Geolocation of Nodes

Technique: This is one of the most straightforward and widely used methods: take the IP addresses of nodes and look them up in a geoIP database (such as MaxMind or IP2Location) to get a country/city/latitude-longitude estimate. Many tools and dashboards (Ethernodes, Bitnodes, etc.) rely on this. When Ethereum's discovery protocol finds peers, or when one scans the network by trying to ping all possible nodes, you gather a list of IPs and then convert those to locations.

What it Measures: Essentially, it maps nodes to the location of their internet connection. Usually, that equates to the location of the server or device. If a node is running on a cloud in Frankfurt, the IP likely geo-resolves to Frankfurt, Germany. If at a home in California, it might resolve to somewhere in California (maybe the ISP's regional registry). So it measures *network location*, which often (not always) correlates with physical location. It can measure the distribution by country or city fairly directly – e.g., “X nodes in the US, Y in Germany” – this is the data behind statements like “United States hosts 33% of Ethereum nodes” ⁴⁷ or “over 30% of Ethereum EL nodes are in U.S., significant clusters in Washington DC” ⁴⁸. IP geolocation is the source of those kinds of stats.

Accuracy Limits: IP geolocation is imperfect. At the country level, it's fairly good for many IPs (especially static ones in data centers), but errors occur. Databases might have outdated info, or an ISP's registration might show the headquarters address rather than the actual node's location. For example,

some IP ranges might all map to a country where the ISP is incorporated, even if customers are elsewhere. City-level accuracy is worse – many geoIP entries are only accurate to the region or are off by hundreds of kilometers. Moreover, for privacy, some nodes use VPNs or Tor; a node could physically be in one country but the IP appears from another (Tor exit node location, etc.). GeoIP will then misattribute it to the wrong country entirely. We should also note IPv6 addresses – these are harder to geolocate in some cases due to sparser data and different allocation structure.

Typical Failure Modes: *False clustering* – sometimes many nodes could appear in one spot because of how IP blocks are registered. For instance, if a cloud provider in one country routes traffic through an IP range registered in another country, it could look like nodes are abroad. Also, nodes in small or authoritarian countries might commonly use VPNs, making it seem like those countries have fewer nodes than they do (because the IP shows as, say, in Europe). A notable failure mode occurred historically: looking at Bitcoin nodes, some early studies found odd concentrations because they didn't filter out obvious VPNs or Tor. Another failure is related to load-balancing: multiple nodes might share one IP (through NAT or proxies), so counting by IP could undercount nodes in a region where many share a gateway.

Sources of Error: The geoIP database itself can be a source of error if not up-to-date or if the IP is very new and not in the database. Also, dynamic IP addresses (common for home internet) might be geolocated to the center of a region or to the ISP's base. For example, a node in a small town might geolocate to the state's capital where the ISP is registered, skewing city-level stats. Reverse DNS lookup sometimes is used (some IPs have a hostname that includes location codes or provider info), but if interpreted incorrectly, that can mislead too.

False Precision Risks: It's common to see world maps with dots or exact percentages by country. These look authoritative, but often lack error bars. For instance, if a map shows 100 nodes in China, is that exact? Perhaps some are misdetected (maybe 90–110 would be plausible). Presenting a static map of “current nodes” might not convey how fluid it is (nodes come and go daily). A user might see a country percentage like 31.6% and assume a significance to the tenth of a percent which isn't really there given data uncertainties ⁴⁹. The Probelab team provides weekly charts but notes they rely on a “leading IP Geolocation provider” and only show dialable nodes ³³ – implicitly warning that this is a subset view. They and others emphasize such context in methodology write-ups, but if one only sees the chart, one might not realize, for example, that a large percentage of “Non-cloud” nodes are simply those whose IP couldn't be matched to a provider, not necessarily all home nodes.

Use in Literature: Many reports leverage IP geolocation. The Cambridge CCAF Ethereum analysis shows a map of beacon nodes by country (using their crawler *Armiarma*) ⁵⁰, basically an IP-based geolocation result. They even updated their crawler for better data, implying earlier data had inaccuracies ⁵¹ ⁵². Another example: Chainstack or others have blog posts measuring Ethereum and finding over half of nodes in 2–3 countries – these inevitably used IP geolocation as the backbone. The *flashbots research directions* thread references “Existing work attempts to do this by... triangulating locations based on response times” with an honest threshold assumption ²⁵, which is more advanced (active probing), but simpler existing work uses IP – e.g., Ethernodes which the flashbots paper cited ⁵³. Ethernodes (ref. [13]) likely does IP geolocation; as of 2025-09-01 it reported certain distributions ⁵³. That data is used in the Yang et al. 2025 paper to illustrate concentration along the Atlantic ⁵. So, IP geolocation is fundamental enough that it underlies a lot of known statements and figures.

Cloud Provider Fingerprinting

Technique: This involves determining if a node's IP or network characteristics match known cloud or hosting providers. Many cloud companies have public IP ranges (AWS, Azure, Google Cloud, Digital

Ocean, Hetzner, etc.). By checking an IP against these lists, one can say “this node is on AWS in region us-east-1” or “this node is in Hetzner’s German data center range”. Tools like ipinfo or ipregistry (which ProbeLab used ⁵⁴) classify IPs as cloud/hosting vs residential. Additionally, reverse DNS names can hint (e.g., an IP that resolves to “ec2-54-xx-xx-xx.compute.amazonaws.com” is clearly AWS). Some researchers also use *TLS certificate clues or trace routes* to identify cloud infrastructure.

What it Measures: It measures infrastructure centralization – specifically the share of nodes on major hosting providers versus independent networks. Geographically, it also often gives a region – clouds have regions (like AWS us-east, AWS eu-west, etc.). For example, an Ethereum node might be identified as “AWS, Virginia (US-East)” which tells us both that it’s on a single company’s infrastructure and in a specific geography. Cloud fingerprinting, combined with geoIP, results in stats like “X% of nodes are hosted on AWS in the US” or “only Y% run outside of cloud data centers”. Indeed, CryptoSlate reported **~37% of Ethereum execution layer nodes on AWS** ¹⁹, based on Ethernodes data which in turn uses IP-to-cloud mapping. Polygon’s team noted over half their validators on just AWS and Hetzner ¹⁰, which they likely got by such fingerprinting.

Accuracy Limits: Identifying large providers is relatively straightforward because of known IP ranges, but smaller or regional providers may not be catalogued, and could be misclassified as “non-cloud” (when they are just a small hosting company) or vice versa. Some node operators also intentionally use lesser-known providers or frequently change hosts to avoid detection. If a node is on a **residential ISP**, fingerprinting might label it “Non-cloud” – which is technically true (not a cloud), but from a decentralization perspective we might want to distinguish *truly independent/home* vs *just a smaller hosting firm*. These nuances can be lost if the classification is binary (cloud vs non-cloud). Also, if a cloud provider uses another’s infrastructure (white-label or resale), one might not realize two seemingly independent data centers are actually related.

Typical Failure Modes: A common challenge is that IP mapping to cloud sometimes lags behind – new data center IPs might not yet be in databases. Also, nodes can be behind content distribution networks or DDoS protection, making them appear to be at an edge server (cloudflare, etc.) which might wrongly be counted as “cloud node” when it’s just protected by a service. In multi-cloud or hybrid setups (some operators use services like Akash or flux which distribute across clouds), fingerprinting might identify the cloud hosting the gateway rather than the actual node.

Sources of Error: Misclassification is the big one – e.g., some IP blocks can host both cloud instances and ISP customers (rare but possible if IP space is subleased). Also, not all cloud providers publish region info in IP whois; sometimes one only knows it’s AWS but not which region (though often hostname or ping latency can hint). If not careful, one could double-count – e.g., if a node has multiple IPs (some nodes might be multi-homed), it could appear on two provider lists.

False Precision Risks: Presenting “N% cloud vs non-cloud” as a single number glosses over uncertainty like how many couldn’t be classified. For instance, ProbeLab’s weekly report shows a pie chart of nodes on known cloud vs not ³⁴, but they likely treat “unknown hosting” as non-cloud or exclude them. If that’s not clarified, one might think all nodes were classified. Also, saying “Hetzner = 15%, AWS = 20%...” suggests exactness, but maybe \pm a few percentage points might be within error if some IPs are borderline cases. Moreover, the presence of a node on a cloud doesn’t tell the whole story of decentralization, but an uninformed reader might conflate “on AWS” with “controlled by Amazon” (not true, but it means reliant on Amazon’s uptime). Communicating what this means needs care.

Use in Literature: This approach is common in blogs and industry reports. The Messari report explicitly measured validator distribution across node hosting infrastructure for several PoS networks ⁵⁵ ¹³, meaning they fingerprinted cloud vs bare metal. They cite that “two major cloud providers – AWS and

Hetzner – power more than half of Polygon nodes” ¹⁰ , indicating such analysis. Academic work also notes it: the Ethereum decentralization simulation paper mentions validators clustering in certain regions partly *because of efficient inter-datacenter links* ⁵⁶ – implying many validators are indeed in datacenters. While that paper doesn’t explicitly list cloud stats, it cites the concentration and uses a metric where they had to define what constitutes independent failure domains, likely considering cloud regions. Community websites like ethernodes provide a “Hosting” breakdown, showing by provider (as referenced in CryptoSlate’s article including an Ethernodes screenshot with AWS 37% ¹⁹). That data drives home the point that even if nodes are spread across countries, they might still reside in just a few companies’ servers.

Latency Triangulation and Active Probing

Technique: By measuring network latency (round-trip times) from multiple vantage points to a node, one can infer the node’s approximate physical location. The idea is if you ping a node from say New York, London, and Singapore, the time differences can constrain where the node could be (like drawing circles of possible distances). This is akin to how GPS trilateration works, but using Internet signal delays instead of satellite signals. Researchers have implemented such triangulation under various assumptions. Some advanced versions (like BFT-PoLoc mentioned in the Flashbots salon ⁵⁷ and search results ⁵⁸) use multiple nodes to send coordinated challenges and use the differences in response times to compute location with certain confidence, even in adversarial conditions (hence “Byzantine Fortified”).

Active probing also includes traceroute-based geolocation – where one traces the route to the node and sees the intermediate hops and their known locations (often routers have city-coded names). Another approach is to use *landmarking*: measure latency from node to a set of servers with known locations (landmarks) to estimate distance. This is like the “Ping triangulation” that some tools (like ripe atlas measurements) do for IPs of unknown location.

What it Measures: This tries to measure physical proximity in terms of network distance, which correlates with geographic distance. It can often narrow a node down to a region or at least a country, especially if some latency measurements are significantly lower from one region (implying the node is likely near that region). It essentially measures how far a node is from known points, which is an indirect map coordinate. Some systems achieve kilometers-level accuracy under good conditions (the cited GeoPoRet scheme in 2021 achieved radii ~1000 km for proofs ⁵⁹ – not pinpoint but region-level).

Accuracy Limits: Internet latency is a noisy measure of distance because routes are not straight-line – they depend on network topology. For example, a node in South America might have a shorter ping to a server in North America than to one in Europe, but undersea cable routing or congestion might introduce anomalies. Additionally, nodes can intentionally delay responses to throw off measurement. Honest measurements assume nodes respond as quickly as possible. If a node operator suspects they are being located, they could add jitter or use relays. BFT-PoLoc assumes a fraction of nodes are honest to anchor timing ⁶⁰ . Without such assumptions, a single node could cheat your probes.

Also, the number of vantage points matters – need enough and well-distributed. If all your ping stations are in one continent, you’ll poorly locate a node elsewhere. This method tends to work best for cooperative scenarios or in research contexts, but doing it at scale for thousands of nodes is complex (requires a network of measurement servers).

Typical Failure Modes: If the network conditions are variable, measurements might misestimate distance (e.g. a temporarily slow link might make a close node seem far). Triangulation can give false results if the node’s traffic is not taking direct routes. For instance, some regions route traffic through

hubs (a node in one country might actually respond via an ISP hub in another, skewing latency). If the node is on a content delivery or DDoS network, you might just be measuring to the edge node, not the actual server – completely throwing off location. Another common failure is *coarse granularity* – you might only confidently place a node in say “Western Europe” not specifically France vs Germany, if latencies to landmarks in those countries are all similar.

Sources of Error: Clock sync issues (if using one-way delay instead of round-trip, but usually round-trip avoids needing sync). Use of ICMP vs TCP ping – some nodes or their host networks might prioritize or deprioritize certain traffic, affecting measured latency. Additionally, many nodes won’t respond to ICMP at all (ping blocked), requiring maybe application-layer pings (like sending Ethereum protocol pings). That complicates things and may have different handling.

False Precision Risks: Triangulation outputs a coordinate or region – it can be tempting to plot a node on a map exactly where the math says. But that might give a false sense that we “found it here”, whereas practically there’s an uncertainty radius. Without showing that uncertainty, one might believe a node is in City X when it could be anywhere within 500 km. If results are aggregated to country counts, similar caution is needed – some nodes near borders or whose latencies fit multiple possibilities might be wrongly assigned. Reporting lots of decimal places from latency-based distance would be clearly spurious; better to bucket it.

Use in Literature: Early academic works on Tor or peer-to-peer network geolocation used such methods (e.g. “Constraint-based geolocation”). In blockchain context, a 2021 work “GoAT: Geolocation via Anchor Timestamping”^{61 62} proposed a proof scheme where nodes use public timestamp servers to help verify location with tolerance ~1000 km. That relies on active timing and trust in some “anchors”. BFT-PoLoc (2024) builds a more decentralized method using many challengers and measuring delays, explicitly deployed on Ethereum and Solana test networks to demonstrate it⁶³. These show academia is exploring this, aiming to make it robust even if nodes lie about timing. The Flashbots reference to triangulating positions with adversarial assumptions⁶⁴ aligns with BFT-PoLoc. Also, in practice, some Ethereum researchers or community (like at Ethstats) have used RIPE Atlas probes to double-check node locations gleaned by IP – e.g., if unsure about a node in Africa vs Europe, measuring latency from African vs European Atlas probes can hint at where it is. The reliability of IP geolocation can sometimes be improved by such latency sanity checks.

BGP and Internet Routing Analysis

Technique: This leverages data from the Internet’s routing system (BGP – Border Gateway Protocol) to infer location or centralization. Each IP belongs to an Autonomous System (AS), often corresponding to an ISP or company network. By looking at the AS of node IPs, one might identify concentration (e.g. many nodes in AS 14618, which is Amazon AWS). BGP analysis might also reveal if a lot of traffic between nodes passes through certain chokepoints or if certain ASes could isolate the network by dropping traffic. In terms of geography, ASes can be mapped to countries (since ISPs are often national or regional). One can also analyze if multiple nodes share the same AS, implying they might be topologically close. Another angle is *BGP announcements*: see if nodes are reachable only via certain internet exchanges or if certain countries could cut off routes to them.

What it Measures: It measures centralization in the Internet topology underlying the blockchain. For example, if 50% of nodes are in ASes that are all owned by U.S. companies, that’s a kind of centralization (both corporate and geographic if those ASes operate mostly in the U.S.). It also can measure dependency: maybe all validator nodes rely on connectivity through a handful of Tier-1 ISPs or undersea cables. BGP analysis can highlight if taking down one AS (or one country’s internet) would

disconnect a large fraction of nodes from the rest. So it's a measure of **network resiliency and diversity** at a level below the application.

Accuracy Limits: Matching AS to geography is approximate – big ASes like Comcast span a country, others like Level3 (CenturyLink) are global. So “AS location” might be too crude. But you can at least identify if an AS is domestic or international. Data for BGP is widely available (e.g. public route dumps), but understanding which nodes specifically depend on which routes can be hard without active tests (like trace routes). If you trace route from one node to another, you might see paths going through major hubs (like a lot of transatlantic blockchain traffic likely goes through the few big undersea cables landing in New York or London). BGP doesn't directly show cable routes, just AS hops, but AS often implies region (e.g. an AS that is the London Internet Exchange suggests traffic exchanged in London).

Typical Failure Modes: AS attribution can mislead if an AS is very large or multi-country. Also, some nodes might be multi-homed (connected to multiple ISPs), which is great for reliability but complicates analysis – which AS do you count it under? Another failure is focusing too much on BGP for censorship analysis – some argue nation-states can do more than just BGP hijacks (they can also seize servers or cut power, which is outside BGP scope). So BGP analysis alone might undervalue threats like legal seizure.

Sources of Error: If using databases to map AS to owner and country, those can be outdated due to mergers or policy changes. Also, BGP announcements change – a route available today may vanish tomorrow if ISPs reroute, which could change which AS looks critical. Temporal changes might cause one to misidentify a permanent central point when it was a transient condition.

False Precision Risks: Saying something like “85% of nodes are reachable only via AS X” sounds specific, but if that's based on limited vantage routing tests, it might not account for alternate paths. BGP-centric metrics (like counting AS diversity) are useful but might be overemphasized if presented as the sole decentralization metric (someone might say “we have an AS Nakamoto coefficient of 4” – meaning you'd need to corrupt 4 ASes to isolate the network). Without context, this could be misinterpreted by non-experts.

Use in Literature: In 2018, Gencer et al. examined network-layer decentralization in Bitcoin/Ethereum, including overlay connectivity and likely some AS analysis ⁶⁵. They found Bitcoin's network (back then) had a handful of ISPs hosting a large chunk of nodes, if memory serves. More recently, papers like “Ethereum's P2P network has a privacy issue” (USENIX 2025) ⁴⁶ likely looked at AS-level data to deanonymize validators – effectively using the network-level footprint (which AS, what latency patterns) to link identities. That implies knowledge that certain ASes or network paths correlate with certain stakers. The Flashbots posts don't explicitly mention BGP, but their emphasis on physical distance implicitly relates to how networks route (latency and BGP are tied; shortest path routing tends to align with geography). We also have anecdotal evidence: after some outages, analyses appear (e.g., “which ISP had trouble such that many nodes dropped?” – I recall during a major German internet outage, many Ethereum nodes went offline because they were on that ISP). These kinds of incident analyses lean on BGP/AS info.

Active Probing of Nodes (beyond latency)

Technique: This can include anything from port scanning nodes for open services, to sending custom queries to extract metadata. For example, an active probe might ask a node for its peer list (some protocols allow this) – those peers could hint at location (if many peers are known to be in one area, maybe the node is too, since networks often prefer nearby peers for low latency). Another probe might

be measuring bandwidth or throughput to a node – if a node has very low latency to a known data center, it might be co-located there.

There's also a concept of **"hitting timing protocols"**: e.g., if a blockchain uses NTP (network time protocol) or other time servers, and one could observe which time server it contacts, that might hint region (some OS choose regional NTP pools). Such indirect probing is esoteric but possible.

What it Measures: These methods measure various side signals that can correlate with location. E.g., traceroute we mentioned yields intermediate hop info; if you see an intermediate router named "sydney.telstra.net", you know the path went through Sydney, implying the node is likely in Australia. Or if a node is using a particular DNS resolver known only to operate in, say, Spain, that hints the node's local environment is Spanish.

Active probes can also identify cloud instances by checking for certain open ports or default server names. For instance, many cloud VMs have a link-local address for metadata (169.254.169.254) – though you can't directly query that externally, you might ask the node to do something that reveals if it's on AWS. One technique: asking a node to download a file from a known fast server and timing it – if it's extremely fast, perhaps the node is in a big data center with good backbone; if slow or inconsistent, maybe a residential line.

Accuracy Limits: These are generally heuristic and can be unreliable. They work best when combined with other data. Many active probes might not be supported by the protocol – you risk being intrusive or even illegal (aggressive port scanning can be seen as attack). There's also an ethical limit: trying to force nodes to reveal info they don't naturally reveal to a line.

Typical Failure Modes: If a node is hardened against scanning, you may get nothing or be blocked. The inferences drawn can be wrong – e.g., a node might have mostly European peers simply by chance or bootstrapping order, not because it's in Europe, yet one might infer it's European. Or maybe a US node connects to many European nodes because US ones were offline at that moment.

Sources of Error: Misinterpreting data – e.g., intermediate routers sometimes have misleading names (a router name might contain "lon" but actually be in "Long Island" not "London"). Also, active tests done at one time might catch the network in a non-representative state (like during a regional outage).

False Precision Risks: Active probing might yield very specific-sounding clues ("the node's traceroute went through 8.8.8.8 (Google DNS) which often indicates it's using Google's network, hence likely in Google Cloud region X"). Presenting such conclusions without probability can be overconfident. These inferences should ideally be labeled as *inferences*, not facts.

Use in Literature: The "File Geolocation via Anchor Timestamping" (GoAT) paper ⁶¹ ⁶² essentially is an active scheme where a node interacts with *public timestamping servers* (which are distributed globally) to prove it's near some of them. That's an elaborate active protocol beyond just measuring. It shows that by active challenge, one can get cryptographic assurance of location (to a bound) if assumptions hold. BFT-PoLoc is similar in spirit but with a security model. These are not everyday measurements but research prototypes that might influence future network designs (imagine a blockchain where validators periodically produce a "proof of location" along with their blocks – not currently done, but conceptually feasible).

Less formally, some community researchers on Ethereum have used active ping and traceroute methods. For example, one thread on ethresear.ch talked about *estimating validator decentralization*

using p2p data ⁶⁶ – likely Bostoen & Garg (2024) – which presumably includes active requests to Ethereum’s discovery protocol to map out which ENRs (node records) correspond to which subnets and geographies. Those approaches often involve actively crawling the DHT and then maybe pinging each found node.

Metadata and Side-Channel Extraction

Technique: This grabs any auxiliary information that might hint at location. Metadata could be: - Node client versions and configuration (some clients might default to connect to nearest region services). - In blockchains like Filecoin, miners might embed an “ask” with data that includes location (not sure if they do, but they might for retrieval). - Public profiles: if a node’s public key or address is associated with a forum username, and that user has said “I operate a node in X”. - DNS-based nodes: Some networks allow nodes to be referenced by DNS names (e.g. P2P DNS seeds). A DNS name like `node-us-east.mychain.com` is a giveaway. - Application layer metadata: For instance, Bitcoin nodes have an address broadcast (ADDR messages) where they relay peers they know. If a node consistently relays peers from a certain /16 subnet more often, it could be near them (this is speculative, but network locality can appear). - Timing patterns: a subtle side-channel is block propagation timing – e.g., if one measures how quickly different known nodes received a block, one might deduce relative distances (used in some deanonymization attacks).

What it Measures: These tend to measure indirectly and can strengthen other findings. For example, if an Ethereum validator’s node is often connected to a particular set of peers that we know are European, that could indicate it’s also European. If a miner in Filecoin always proves storage around a certain time consistent with a timezone, one might guess location (though that’s weak).

Accuracy Limits: This is quite hit-or-miss. Some nodes will simply have no extra metadata. Others might intentionally obfuscate. The accuracy of any inference depends on pattern consistency and assumptions (lots of chance for false correlations).

Typical Failure Modes: False correlations (assuming a relationship that isn’t causal). If someone tries to use social media (e.g., “Twitter user says they run a node in Tokyo”), that’s manual and not scalable, plus not always reliable. Also, nodes can change behavior or peers over time – what was true last week may not hold if network topology changed or after a restart.

Sources of Error: Human error in linking identities, and noise in network behavior. For example, the Ethereum peer-to-peer network is random enough that local peers are not guaranteed – an Australian node can still connect to a U.S. node easily. So seeing it connected to a U.S. node doesn’t necessarily mean it’s not in Australia.

False Precision Risks: If one claims “we identified X node’s operator is likely in city Y because of metadata Z,” there should be an asterisk unless it’s very direct metadata. Overstating these can be embarrassing if proven wrong by later info.

Use in Literature: There’s some precedent: for instance, the 2018 IMC Ethereum paper by Kim et al. found some nodes by exploiting the Kademlia protocol specifics, essentially using the network’s gossip to find more nodes and maybe grouping by subnet ⁶⁷. They might have also looked at client IDs – if a certain client is more popular in China (say a Chinese localized client) that might hint some distribution. But that’s second-order. Another example: rated.network and Labrys tracked OFAC-censoring relays on Ethereum – those relays are specific servers, often U.S.-based companies, which they identified by name ⁶⁸. That’s not exactly node location, but it’s actor location which is tied to censorship.

In sum, every technique from basic IP mapping to advanced triangulation provides a piece of the puzzle. Their **accuracy varies** – often country-level accuracy is achievable with moderate confidence (especially if multiple methods agree), whereas pinpointing city or data center often requires either luck or extraordinary effort (and even then might be wrong). Each method has **failure modes**, so the best practice, as we'll later synthesize, is to combine them, cross-check, and always be clear about uncertainty ⁴.

Before leaving this section, it's worth noting that combining techniques has already yielded insights. For instance, Ethereum's current state analysis uses IP geolocation for broad stats ⁵, cloud fingerprinting to highlight reliance on a few providers ¹⁹, and latency-aware simulation to predict what would happen if incentives change ⁷ ⁴². Each complements the other. And security critiques remind us: **if an attacker or authority wanted to find nodes, they could also use these methods**. In fact, one reason to study them is to understand what an adversary could know about the network's geography, which influences threat models (for example, if all top validators can be found in one country, an adversary in that country has a clear target list). This dual-use aspect underscores why accuracy and honesty in measurement are important – both for defense (improving decentralization) and awareness.

3. How Major Protocols Measure and Discuss Decentralization

Different blockchain communities place varying emphasis on geographic decentralization, and their approaches to measuring or ensuring it can be discerned through public metrics, research, and sometimes internal commentary. We will examine several major protocols: Ethereum, Bitcoin, Solana, Cosmos, Filecoin, Polygon (as a prominent sidechain/L2), and others like layer-2 networks, focusing on: - What metrics or evidence they provide on decentralization (especially geographic). - What aspects they avoid or understate. - Differences between their public narrative and any known internal concerns. - External analyses or papers critiquing their decentralization.

Ethereum

Public Metrics and Communications: Ethereum, especially since its shift to proof-of-stake, has seen active discussion on decentralization. Publicly, one often-cited metric is the number of nodes and their distribution. Websites like Ethernodes and Etherscan's node tracker give real-time stats on node geographic distribution. For example, Etherscan's "Ethereum Node Tracker" (as of recent data) shows the top 10 countries hosting nodes – usually U.S. and Germany leading by a large margin ⁴⁹ ⁶⁹. This is part of the narrative that Ethereum is a global network (albeit one dominated by a few countries). The Ethereum Foundation's website doesn't overtly emphasize geography in its definition of decentralization, focusing more on client diversity and stake distribution; however, EF researchers and core developers have raised concerns about geography in various forums.

One public communication highlight: **Ethereum's All Core Developers (ACD) calls** occasionally touch on network health. In late 2022, after The Merge, there was scrutiny of how many validators were U.S.-based or using U.S.-based services (due to the OFAC sanctions issue). While not official EF pronouncements, figures like Vitalik Buterin and others have acknowledged that having too many validators in one country (or on one provider like AWS) is problematic for censorship resistance. The community created dashboards like **MEV Watch** to track the percentage of blocks being built by OFAC-compliant relays (which indirectly measures how U.S.-influenced the network is). At worst, this reached ~60–70% blocks censored ⁷⁰ ⁷¹, raising alarm publicly on social media and crypto news. Ethereum's public ethos is strongly against censorship, so this metric was and is tracked closely until it improved (by late 2023, OFAC-compliant block percentage reportedly fell to ~27% ⁷² as more non-censoring relays gained share).

In terms of node distribution, Ethereum's public explorers show a **heavy tilt to the US and Europe**. One real-time map highlighted by community members showed this clearly, prompting commentary that decentralization "isn't where it should be" (some articles pointed out that even though there are nodes worldwide, two countries dominate) ⁷³. However, Ethereum leadership often emphasizes other forms of decentralization (client/software diversity, governance openness) more than explicitly saying "we need more nodes in Africa or Asia."

Internal Concerns and Actions: Internally (in research and dev discussions), geographic decentralization is a pressing topic. The Flashbots "Geographic Decentralization Salon" at SBC 2025 was heavily focused on Ethereum's case ⁷⁴ ⁷⁵, with talks about Ethereum data and simulations. This indicates that within Ethereum research circles, they are actively measuring and worrying about it: - One talk was "*Geo Decentralization & Ethereum: A Data Perspective*" ⁷⁶. This likely covered current metrics like block propagation delays across regions, MEV effects on different continents, etc. The fact that it's first on the agenda shows Ethereum is a prime case study. - Another talk by Flashbots researchers "*Simulating Centralization*" ⁷⁷ deals with modeling changes in Ethereum's design and how that affects validator location incentives (we know from Yang et al. 2025 paper that they simulated Ethereum under different block-building paradigms and found North America consistently becomes a hub without interventions ⁷⁸ ⁷⁹). - Phil's talk "*Defining Geographic (De)Centralization*" ⁸⁰ suggests Ethereum is used as an example when contrasting protocols. Indeed, Phil's definition (latency sensitivity metric) was arguably inspired by Ethereum's latency constraints (12 second slots, need 2/3 attestation by ~4s). Ethereum's design, such as Proposer-Builder Separation (PBS) and slot timing, is being scrutinized for its centralization pressure on geography ⁷ ⁸¹.

The Ethereum community also had concern after the Merge that staking became dominated by a few pools (Lido, centralized exchanges) – not a geography issue per se, but it intersects: e.g., Coinbase and Kraken staking largely means U.S.-based legal entities controlling many validators. Lido's node operators are more spread out (some in Europe, some in US, some elsewhere), but it still introduced the worry that if regulators targeted those entities, a big chunk of validators might comply with censorship. On internal channels (Ethereum research forums, etc.), there have been proposals such as **encouraging home staking** (to boost geographic and ownership diversity) and **lowering hardware requirements** so that more people in varied places can run full nodes. Vitalik's writings often champion light clients and decentralizing infrastructure, though not often framed explicitly as "geographic" decentralization, it implicitly is (make it easy enough that someone in a developing country with a normal laptop can validate, and you'll naturally get more global distribution).

One specific internal effort: **DiscV5 crawler by Probelab** (affiliated with Ethereum Foundation and others) – they have a sustained effort monitoring node counts by country and cloud weekly ⁸² ³³. The existence of that and integration into CCAF's index ⁵¹ indicates Ethereum's stewards care about tracking this over time, not just a one-off.

Critical Papers & Controversies: Academia has kept an eye on Ethereum. The 2018 paper by Gencer et al. already noted that Ethereum (back then PoW) had more nodes in the US than Bitcoin did, showing centralization in that aspect ⁴⁴. In 2019, a paper by Kwon et al. "Impossibility of full decentralization" used Ethereum as an example where despite many nodes, network propagation and incentive quirks lead to centralization trade-offs ⁸³ ⁸⁴. A 2021 study "Measuring Decentralization in Bitcoin and Ethereum using Multiple Metrics" likely went through geographic metrics among others ⁸⁵. More recently, the 2024/2025 works by Heimbach et al. (IMC 2023 and USENIX 2025) found ways to deanonymize Ethereum validators ⁴⁶, revealing that you *can* pinpoint many validators' IP addresses (which means location). Those works likely highlight, perhaps uncomfortably for Ethereum, that a large fraction of validators were on identifiable hosting (somewhat centralizing network-wise).

Another point of controversy: **Reducing Ethereum's slot time** (from 12s to maybe 1s as per EIP-7782) has been debated. One big argument against faster slots is it could disadvantage geographically far validators (less time to propagate blocks). Quintus in Flashbots forum noted discussions around slot time making geo decentralization "more pressing" ⁸⁶. And indeed the simulation in Yang et al. Appendix O.E.4 found that going to 3s slots doesn't drastically change centralization, but it does increase reward disparity a bit ⁸⁷ ⁸⁸. The fact they studied this suggests Ethereum's core developers are concerned how protocol changes impact geography. Publicly, Ethereum hasn't yet reduced slot time, partly due to these concerns – an internal recognition that too-low latency requirements could force validators to cluster (e.g., all near New York if New York becomes an MEV hotbed). So Ethereum's approach is to **study and be cautious**.

Summary for Ethereum: Publicly acknowledges being global but also shows data that a few regions dominate. Internally, actively researching how to improve (or at least not worsen) geo-distribution. Critical observers point out issues like reliance on U.S. jurisdiction (e.g., the fact that the U.S. Treasury could affect Ethereum at all was a wake-up call) and reliance on a few cloud/ISP providers ¹⁹ ²¹. There's controversy especially around MEV and PBS – Flashbots' relay centralized block distribution initially, arguably making a focal point (the Flashbots relay mostly in US) that worried people; they've since decentralized the relay ecosystem somewhat.

Bitcoin

Public Metrics and Communications: Bitcoin, as the original decentralized blockchain, often touts the number of full nodes (and encourages users to run their own). However, Bitcoin Core developers historically haven't provided a lot of official data on node geography. Instead, independent sites like **Bitnodes.io** track reachable nodes by country. As of recent data, the US and Germany often top the list for Bitcoin nodes – for example, one source in 2023 indicated roughly 30% in USA, 20% in Germany, then countries like France, Netherlands, etc., each under 5-10%. This is commonly known in the community but not heavily advertised; Bitcoiners tend to argue that as long as anyone anywhere can run a node, the exact distribution is less a concern. The focus for Bitcoin has been more on mining decentralization and censorship resistance of transactions.

However, **mining** is where Bitcoin's geographic story is more dramatic. Public communications often referenced the **Cambridge Bitcoin Electricity Consumption Index (CBECI)** which, until recently, tracked mining hash power by country. For years, China was over 50-60% of global hash (not publicly trumpeted by Bitcoin officials, but widely known) ⁸. In mid-2021, after China's ban on mining, Bitcoin folks proudly noted how the network hash rate dropped then fully recovered as miners relocated – a vindication of resilience. Now the distribution shifted: the US reportedly became the largest (around 35% by early 2022), with Kazakhstan, Russia, Canada next. These figures were used to demonstrate improved decentralization vs the China-heavy era, but also raised new concerns (e.g., the US share – could regulation or outages in the US have big effects?).

On node decentralization, Bitcoin's design (10 minute blocks, simple transaction relay) is more forgiving to geographic latency than Ethereum's fast finality requirements. So publicly, Bitcoiners often say any geographic distribution is fine and point out that Bitcoin blocks propagate globally in a few seconds out of 600, so being far apart isn't an issue for security (just maybe a slight increase in orphan risk). There is an initiative called **Galaxy's Mining reports** and others that talk about how many mining pools are in which country, etc., but Bitcoin Core maintainers rarely discuss geography explicitly.

Internal Concerns: Within Bitcoin dev mailing lists, one area of concern has been **network topology** – specifically, the reliance on a few ISPs or the risk of partition. Research by Ethan Heilman et al. in 2015 showed that a large portion of Bitcoin nodes' traffic went through just a few ISPs and internet

exchanges, creating potential choke points. This led to discussions on diversifying connections (Bitcoin added some *relay networks* like Fibre to speed block propagation and reduce orphan risks globally). Also, efforts like **Satellite Bitcoin** (Blockstream's satellites broadcasting blocks) were partly to ensure even if the internet is partitioned, anyone with a dish globally can still get blocks – this addresses geographic resilience indirectly.

Mining decentralization in Bitcoin has been debated: while pools are used (which can centralize control), it's often pointed out that pools are geographically distributed entities – e.g., even if Foundry USA pool has majority hash, the actual miners are across states or countries. But then policy like OFAC could pressure that pool. Indeed, in 2020-21 there was talk about pools like Marathon intending to mine OFAC-compliant blocks (they later backed off). So Bitcoin's community watches geography mostly in context of nation-state interference. After China's ban, there was both relief (network survived, diversified) and new caution (don't let any one country, even the US, get too dominant).

Internal actions to promote geographical spread are not as visible as Ethereum's. Bitcoin's design is pretty static; no parameter like slot time to tweak for geography. Instead, initiatives are more grassroots: encouraging node operation globally (there are projects to translate Bitcoin documentation into many languages, NGOs distributing nodes, etc.). The **Global South** is sometimes mentioned – there's interest in more nodes and mining in Latin America, Africa for true global adoption. But metrics on how well that is going are scant. (One anecdote: a Brazilian exchange runs thousands of Bitcoin nodes to boost the count in Brazil, which artificially inflates node count; that kind of behavior can skew any geographic metric).

Critical Papers & Points of Controversy: Academic works have pointed out some centralization: - Gencer et al. (2018) found that at that time a majority of Bitcoin nodes were in just 3 countries (likely US, Germany, France) – they gave stats similar to Ethereum's 43% US in Ethereum vs 30% US in Bitcoin in 2018 ⁴⁴. So Bitcoin had more geographic spread among nodes than Ethereum then, but still, US was a large chunk. - They also pointed out mining pools made Bitcoin's "control decentralization" much less than node decentralization. That's a different dimension but relevant (Chinese pools controlled >50% of hash, etc.). - There have been papers on Bitcoin network delays and partition attacks (e.g., where a malicious ISP could delay block propagation to certain regions causing fork issues). Those highlight reliance on certain internet paths.

A controversy that flared was the claim "~60% of Bitcoin full nodes run on AWS" which floated around in media around 2019 (I believe this was an exaggerated claim derived from a faulty analysis). It was disputed by developers but indicated the community's sensitivity to the idea that many nodes might actually just be cloud instances (like people spinning up AWS nodes to increase count). If it were true, that's both infrastructure and geo-centralization. Bitcoin folks contested that, suggesting that many are on small VPS providers or home connections. The reality is unknown because not as thoroughly studied as Ethereum's probe work. Bitnodes suggests a big portion of Bitcoin nodes are in Western countries, but doesn't break down by cloud vs home easily.

One clear data point: **China's ban** was a real-world test of geographic concentration risk. When China banned mining in June 2021, Bitcoin's total hash rate fell by ~50% almost overnight ⁸. This proved that indeed a majority of mining was in China (despite earlier claims that it was maybe lower). The network adjusted difficulty and miners relocated across the globe (notably to North America, Central Asia). Within 6 months, hash rate hit new highs, demonstrating recovery. This event is often cited academically as a case of geographic risk materializing and being mitigated ⁸ ⁸⁹. But it also underlined that "decentralized" Bitcoin had an Achilles heel: one government temporarily slashed capacity in half. Now with ~35% in US, one wonders if a coordinated regulation (like heavy taxation or constraints on mining) in the US could do similar (less likely given US political structure, but possible).

Bitcoin's design meant it survived such a hit by design (no liveness threshold needed like 2/3; even if 30% of miners remain, blocks just come slower until difficulty adjusts).

Summary for Bitcoin: Publicly, it upholds decentralization but doesn't emphasize geography explicitly, except to celebrate that it's spread enough that no single authority can kill it. They highlight events like China ban survival as evidence of resiliency. Internally, improvements focus on network robustness (satellites, relay networks) rather than direct geographic balancing. Critiques point out that mining and node distribution still cluster (in wealthy regions with cheap power or good internet). Some controversies have been around how centralized mining pools or certain geographies got, but Bitcoin's answer is usually that market forces will correct extremes (as arguably happened after China's ban).

Solana

Public Metrics and Stance: Solana is a high-performance Layer 1 that has faced scrutiny over its decentralization. Publicly, Solana Labs and the Solana Foundation have at times released stats about their validators – number of validators, Nakamoto coefficient (Solana's Nakamoto coefficient is often cited around 19–30 for different aspects like stake, etc.). They do mention geographic distribution occasionally. For example, a 2022 Solana blog might note validators in “over X countries”, etc., to assure it's not just run by a small group. One can find on Solana's blockchain explorer some data – previously, it was noted many Solana validators were in data centers in **Germany and the US**. In fact, one known issue: **Hetzner** (a German hosting provider) historically hosted a large fraction of Solana validators (and also Ethereum and others). In late 2022, Hetzner declared crypto-related usage against its terms, raising alarm. At that time, roughly 40% of Solana validators and a similar chunk of new Ethereum validators were on Hetzner (with a lot in Germany). This was widely discussed on Twitter and crypto media as a centralization risk (and a live one if Hetzner kicked them off). Solana's team likely took note; indeed, soon after, the Solana Foundation started initiatives to get validators on more diverse cloud providers and regions.

Solana's network health report (if any) or semi-official community sources (like validators.app or Solana Beach) track how stake is distributed across validators, and some have info on data center or country. As of mid-2023, reportedly, the top countries for Solana validators included the US, Germany, and a few others – similar to Ethereum's distribution but with maybe even more in Europe relative to size.

What They Avoid: Solana often focuses on *performance metrics* in public comms (TPS, etc.) and less on decentralization in terms of nodes. They faced critique that their hardware requirements (very high) make it so only validators in data centers with strong hardware can run, implicitly reducing geographic and demographic diversity. The Solana folks usually respond that throughput demands that, but they have a lot of validators (~2000) which is more than many proof-of-stake chains, hence “decentralized enough” in their view. They seldom brag about “anyone can run a node on a Raspberry Pi” – because you can't for Solana. So there's a bit of defensive tone: they might emphasize the quality of validators rather than quantity or global spread.

Internal/Community Concerns: The community did raise the Hetzner issue strongly – it was a wake-up call that too many nodes on one provider is bad. The Solana Foundation then introduced a program possibly to **incentivize validators to use other cloud providers or regions** (I recall something about server credits or guidance for new validators in different locales). There's also been talk about more Solana validators in Asia and South America – because a lot are in US/EU currently. The network outages Solana experienced in 2021-22 weren't directly due to geography, but some argue if validators had been more spread and not mostly on the same few clouds, maybe some bugs wouldn't have hit everyone simultaneously (debatable).

Academic or third-party analysis: In 2022, Messari's report (we have the 2023 one ⁵⁵ ¹³) included Solana. They noted Solana's **operational decentralization** issues – e.g., a high Nakamoto coefficient for consensus (maybe ~31 for Solana stake at the time), but heavy infrastructure concentration (many on Hetzner or OVH). They likely pointed out that despite 1,900 validators, a lot of stake is on a subset of them and physically in a few places. Also, Solana's **energy use** and high hardware might tether it to developed regions with good electricity and cooling.

A controversy: Solana's choice to use **Google Cloud** for its block explorer and some RPC nodes – people jabbed that “Solana went down because Google Cloud had an issue,” though that was more about front-end services, not consensus. But it highlights perception that Solana is heavily tied to big tech infrastructure.

Critical commentary: Researchers and rival communities often note that Solana's design (Proof of History and high throughput) inherently centralizes because it requires high-end machines in good network hubs. The Solana team counters that they are increasing validator count and can lower hardware requirements as tech improves (like optimizing client). Meanwhile, they have improved documentation for anyone to try running a validator (but realistically, it's still tough outside data centers with gigabit connections).

Summary Solana: Publicly acknowledges distribution but tends to gloss over that many are in a few data centers; instead, emphasizes absolute number of validators and Nakamoto coefficient (which is one of the better ones among new L1s, in the 20s, meaning ~20 validators control 33% of stake or so). Internally, taking steps to diversify after scare with Hetzner. Externally criticized for effective centralization due to infrastructure homogeneity (which has a geographic dimension – many validators in just 2 countries).

Cosmos (and Tendermint chains)

Public Metrics: Cosmos is a network of independent blockchains (zones) each with their own validator set. The **Cosmos Hub** (ATOM) itself has ~175 validators (max limited by protocol). Many other zones have 50-100 validators. Cosmos folks often highlight their **Validator diversity**, but much of it relates to stake distribution and who the validators are (names like stake.fish, etc.) rather than geography. However, because Tendermint BFT requires >2/3 online for liveness, they are acutely aware that correlated outages matter. There have been instances of Cosmos zones halting because a datacenter outage took >33% of validators offline. E.g., in 2022, an OVH (French cloud) outage caused some Cosmos chains to halt because a chunk of their validators were using OVH in that region. This taught Cosmos communities to try to diversify hosting.

Some Cosmos blockchains have maps on their explorers showing validator locations (if the validators provide that info or can be inferred). The **Cosmos Hub** hasn't, to my knowledge, published an official geo breakdown of its validators in numbers. But informally, many Cosmos validators are in Europe and North America, with a few in Asia-Pacific. It's somewhat limited by who participates (tends to be crypto companies or enthusiasts mostly in tech-centric regions).

What They Avoid: Cosmos marketing tends to be about interoperability and sovereignty; they don't often talk about geographic decentralization in the way Ethereum or Bitcoin communities might. Perhaps because each chain is small enough that identifying where each validator is might be sensitive. Also, many validators run multiple networks (there's an overlap where a few professional validator companies validate on dozens of Cosmos chains). This is a centralization vector (if one company in one place fails, it could hit many chains at once). This is not highlighted publicly, but discussed in community (some call for more independent validators).

Internal/Community Concerns: The Cosmos community does have discussions on increasing decentralization: e.g. lowering barriers for new validators (to avoid all stake concentrating on a few, often those run by bigger companies in known regions). But hardware requirements for Cosmos chains are lower than Solana or ETH, so theoretically people anywhere could run. Yet in practice, you need reliable uptime and connectivity to not get slashed, so many use cloud hosting. The Cosmos community is somewhat decentralized; there's no single foundation controlling all zones, but the Cosmos Hub's stakeholders might encourage things like running some validators on different continents by delegating stake to those in underrepresented areas (if that info is known).

One example of concern: **Juno network** (a Cosmos zone) in 2022 had most validators on Contabo (a German cloud provider). When Contabo had an issue, Juno's network had problems. It led to discussion that "hey, we should coordinate to ensure not too many of us use the same provider." This kind of self-organizing is unique in permissioned validator sets, because validators can talk and decide to diversify – something permissionless chains can't directly coordinate.

Critical Perspectives: People analyzing proof-of-stake often point out that fixed-size validator sets (like 100 validators) tend to end up fairly professionalized (on clouds, in data centers). A 2023 paper by Decentral Park or others might have looked at Cosmos Hub and found, say, a certain percent in Europe etc. The Messari report we have included **NEAR and Flow and Aptos** – not Cosmos Hub, interestingly – but other sources likely cover Cosmos. Possibly the Electric Capital validator reports (if any) or community compiled lists exist.

A controversy is that some Cosmos validators are actually on **bare metal servers in one location** for multiple networks – if that data center goes down, multiple networks halt. This correlated risk was realized when a fire in an OVH data center in 2021 took some French-hosted nodes offline across multiple chains. Cosmos chains halting from such events show the stakes of geo/infrastructure clustering.

Summary Cosmos: Not heavily public about geo metrics but aware of risks after some incidents. They rely on social coordination to mitigate (like encouraging validators to be geographically redundant). Each chain's level of decentralization varies. There's an expectation that because validator sets are somewhat small, they might be more easily captured by one jurisdiction's regulations (if most operators in one region). For instance, if 80% of Cosmos Hub validators were in EU and EU passed a law affecting nodes, that could be problematic. This hasn't been tested yet, but is a looming thought as regulations like MiCA in Europe consider nodes.

Filecoin

Public Metrics: Filecoin, being a storage network, interestingly *incentivizes* geographic distribution of data (to ensure redundancy). However, the mining power (storage power) in Filecoin has been historically quite concentrated in China and East Asia. Early on (2020-21), a huge chunk of Filecoin miners were Chinese (due to hardware supply and interest). The Filecoin Foundation published some stats – like how many distinct locations store data for certain datasets, etc., but on miner location, they might rely on self-reporting or IP. I recall that in late 2021, more than 70% of Filecoin's storage capacity was in China. They recognized this as a potential problem (especially after China banned crypto mining broadly, though Filecoin wasn't targeted specifically, it's sort of under the radar).

Filecoin has a concept of *regions* for its notary system (DataCap allocation by region), indicating they want more miners in places like North America, Europe, etc. They have held events to encourage uptake globally. But metrics – possibly on their dashboard or in cryptoeconomics reports – likely show distribution of storage providers by country. If not public, academic references do exist: One 2021

reference (the GoAT paper mention) came as a response to the observation that if all replicas of data are on one hard drive or one city, it's not robust ⁹⁰ . They proposed geo proofs to enforce distribution ⁶¹ . This indicates the Filecoin research community knows geographic redundancy is core to their mission (robust file storage).

What They Avoid: Early on, Filecoin avoided the topic that a few mining farms (some even reportedly colluding on deals) dominated capacity, many in the same area. They framed growth positively – “over X pebibytes of storage” – without highlighting if 50% is in one province in China. However, after seeing what happened to Bitcoin mining with policy, they likely are working to diversify.

Internal/Industry Concerns: There is explicit research like the GeoPoRet (GoAT) protocol ⁶¹ that came from folks like Protocol Labs (Filecoin's core company) to solve proving data is in multiple regions. They want to be able to say to a client: we stored your file on 6 continents. But currently, a miner could claim to replicate data in 6 places but actually keep all copies in one server (just pretending to be different miners). That's a threat to the network's promise. So they are actively investigating how to cryptographically guarantee geographic distribution (which is quite novel; typical blockchains don't try to guarantee geo distribution, they just hope for it).

Protocol Labs people have also talked about decentralization metrics; they are part of the same Web3 space that Flashbots engages with, so they likely cross-pollinate ideas. Possibly, some of the Flashbots forum references (like the [2021] File Geolocation via Anchor Timestamping thread ⁹¹) came from IPFS/Filecoin researchers. That suggests coordination to improve that aspect.

Critical Analyses: Outside observers note that Filecoin's **trusted setup and mining** had high barriers, which resulted in big players mostly in one region. Also that actual useful storage adoption was uneven, not global as intended. If a lot of storage is in one country, censorship of certain content or network availability could become issues (imagine if Chinese miners held most copies of some data and then got cut off – though Filecoin is content-addressed, so copies elsewhere would survive, but bandwidth to that data might drop drastically).

Summary Filecoin: They conceptually value geographic decentralization (for data redundancy) perhaps more than any other, to fulfill their robustness goal. They have tech R&D to enforce it (unique among networks). But current state likely still sees heavy regional clustering. We might expect them to publish improvements – e.g., “Filecoin now has miners in 50+ countries, none over X%” – if they achieve it.

Polygon (and Other Ethereum L2s)

Public Metrics: Polygon (the PoS sidechain) has been more transparent than most about its validator decentralization. The Polygon Labs blog we opened actually enumerated metrics like geographic distribution and cloud distribution of their validators ⁹² ¹⁰ . They proudly pointed out no single country has >1/3 of nodes ⁹ and no single cloud >1/3 ¹⁰ . This is a strong communication: they want to assure that even though Polygon is somewhat permissioned (validators are known and invite-only initially), it's not all concentrated. They listed diversity as a factor and gave specific numbers, which is commendable.

They also listed the Gini coefficients and entropy of stake distribution ⁹³ ⁹⁴ , showing an awareness of multifaceted decentralization. The context was likely to preempt criticism that Polygon was run by a few players or all in one place. Given that blog was 2022, they saw value in being ahead of the narrative by showing “we're not that centralized on these metrics.”

Major L2s (Optimism, Arbitrum, etc.): These are mostly sequences run by one entity (at least as of early 2023). They are inherently centralized operationally (one sequencer node, often on a cloud). However, they plan to decentralize by adding more nodes or making permissionless sequencers. So right now, their geographic decentralization is trivial: if Arbitrum's sequencer runs on AWS in us-east, that's it. But they perhaps have backups elsewhere. They don't talk much about this publicly, because it's a sore point that these L2s are not decentralized yet. Flashbots references did mention "major L2s" in the question – likely meaning we consider them in design, though they won't be in beta index except maybe Polygon (which at least has many validators). Perhaps mention that currently major rollups are *operationally centralized*, so geographic distribution is minimal (e.g., one or two servers), but they aim to improve it. StarkNet, another, similarly has a centralized sequencer now.

Polygon's Avoidance: Polygon acknowledges geographies but what they may not mention is, say, how many validators might be run by the same company or how many are actually just in Europe vs Asia specifics (they did country broad strokes). They also had relatively few validators (100) which can only be so distributed. Also, many Polygon validators might be exchanges or entities in similar jurisdictions (e.g., some of the biggest are Binance, which is mainly global but has presence in multiple countries; a couple of others in US/EU). They perhaps avoid highlighting that some of those validators could be colluding or owned by related parties (just hypothetical).

Internal/Community: Polygon's team clearly thought about decentralization dimensions to have written that article. They likely track these metrics internally each time they add validators. They will soon re-architect Polygon (with their new POL token and multi-chain approach), possibly increasing validator sets or sharding them. They may use those metrics to gauge improvement. The community around Polygon doesn't loudly criticize decentralization because it's known it's somewhat federated (and many users just care about low fees). But as regulators might question if it's decentralized enough (for being not a security etc.), Polygon wants to show metrics in its favor.

Critical Perspectives: Some Ethereum purists or analysts might say Polygon's decentralization is weaker than Ethereum's because it's effectively run by a fixed set of validators many of whom could likely be influenced by Polygon Labs or partners. But at least geographically, their own data shows decent spread (no single country >33% ⁹ which is better than Ethereum where US alone is ~30% and Germany ~15%, combined ~45% > 33%). Cloud reliance >50% on two providers is a risk ¹⁰, albeit each <33%. So by their numbers, they tried to avoid any obvious >1/3 concentration. Possibly they curated validator onboarding to ensure that outcome (e.g., not all validators from one country).

Summary Polygon & L2s: Polygon publicly measured and communicated decentralization including geography, making it somewhat unique among projects. L2s in general currently have a central operator so geographic decentralization is minimal, but in design discussions (esp. for future decentralized sequencers) geography will come. For instance, the idea of multiple sequencers could lead to them being in different regions to improve performance and trust (if one fails, another picks up elsewhere). So the design process might consider latency and region distribution to avoid all sequencers being e.g. on AWS US. However, those projects are earlier in that journey than base layers.

Other Protocols (Lightning, etc.)

The question said consider beyond blockchains, but for brevity: - **Lightning Network (Bitcoin's L2):** It's P2P and many nodes run on Tor. Geographic analysis shows many LN nodes in Europe and NA, but since it's not the main security layer, we won't dig deep. It does face centralization concerns around hubs, which often are in those same areas. - **Ethereum Layer-2s (like StarkNet, zkSync):** similar to Arbitrum/Optimism currently (one sequencer). They might run in specific jurisdictions (e.g., StarkWare is Israeli/U.S., but run on AWS likely). - **Other L1s (Cardano, Avalanche, etc.):** They also have interesting

distributions. Cardano boasts a large number of pool operators globally, with quite some in Europe, US, and a fair number in Japan and other places. Avalanche's validators (over a thousand) are likely mostly cloud too. Each could be its own study, but the broad trend is: most public PoS networks have US and Europe heavy presence with efforts to expand beyond.

Points of Controversy across protocols: Many claim high decentralization until an incident or analysis reveals concentration (like the AWS outage revealed how many were on AWS ¹⁹ ²¹). After such moments, protocols might adjust course or at least community perception shifts. The interplay between *public messaging* ("we're decentralized globally") and *reality* is sometimes stark. For instance, some marketing materials from smaller chains might say "Nodes all over the world" showing a world map with dots – but the reality might be half those dots are cloud instances in a few data centers just with IPs in different countries.

Cross-Comparison and Controversy: There's often debate, "Which network is more decentralized?" e.g., Bitcoin vs Ethereum vs newer chains. Geography is one angle: Bitcoin fans might say "Bitcoin mining now in many countries, whereas Ethereum staking is mostly in US/Europe, plus Ethereum uses a lot of cloud." Ethereum fans retort that Bitcoin mining still has manufacturing centralization (most ASICs made in one country – an *adjacent field* issue, supply chain). Solana's critics say it's geographically and infrastructurally centralized, Solana points to number of validators being higher than many proof-of-stake peers. So each chooses metrics that favor them: - Bitcoin: number of full nodes (though they could be in few places). - Ethereum: number of validators (though many might be hosted by few providers). - Solana: Nakamoto coefficient count (19 or 30, higher than others in stake terms). - Cosmos: number of independent chains and validators variety (though each chain small). It highlights why a comprehensive framework (Section 5) is needed to objectively compare.

To close this section, **points of controversy** often revolve around: - Can a network claim to be decentralized if X% of its nodes/validators are in one country? (This came up with Ethereum and OFAC: some argued Ethereum was under US control; others said it's temporary and being resolved). - Does cloud hosting invalidate decentralization? (Some purists say yes: if all nodes on Amazon, Amazon can theoretically shut them off, so not resilient). - Are newer high-performance chains sacrificing too much decentralization for speed? (Solana is the poster child of this debate). - How to measure multi-chain ecosystems decentralization? (Cosmos: is it decentralized because many zones, or are they each centralized? Polkadot similar question with its parachains and validators).

Each protocol grapples with these and has their own narrative, but independent research like the Flashbots collective and Messari is starting to standardize scrutiny across them ¹³ ⁹⁵ . We will expand on those frameworks in the next section.

4. Insights from Adjacent Fields

Decentralization in Web3 doesn't exist in a vacuum; it echoes concerns in many established fields. By exploring analogous challenges and solutions in other domains, we can glean frameworks and warnings that apply to blockchain networks. Here we draw parallels with telecom, internet infrastructure, content delivery, power grids, supply chains, finance risk modeling, and disaster planning – identifying which concepts map well and which might not.

Telecom Infrastructure Resilience

The telecommunications industry has long dealt with building networks that can survive localized failures. Concepts like **redundant routing**, **last-mile diversity**, and **avoidance of single points of**

failure are key. For example, phone networks ensure multiple trunk lines between major cities so that a cut cable doesn't isolate a region entirely. Similarly, mobile networks use multiple cell towers overlapping so if one tower fails, coverage remains.

Mapping to Web3: Blockchains similarly need redundancy: multiple independent nodes in each region such that if one node fails, users in that region can still reach the network via another. Telecom's principle of *no single point of failure* translates to avoiding situations where one data center or one undersea cable carries the majority of blockchain traffic. An outage of a transatlantic cable in 2008 severely slowed internet traffic from Europe to Asia (via US) – but the internet routed around after some hours. For a blockchain, if most validators were connected only through one cable or ISP, a break could partition the blockchain network (leading to forks or downtime).

Telecom resilience also emphasizes **diversity of providers**: e.g., governments encourage not relying on just one vendor for critical infrastructure. In blockchains, this suggests encouraging that not all nodes rely on one cloud or one ISP (very analogous to the cloud provider issue ²¹ ²²).

One direct inspiration: the idea of **regional NAPs (Network Access Points)** that improved internet robustness can inspire **regional blockchain hubs or bootstrap nodes**. The internet, early on, had critical exchange points; the loss of one (like a MAE-West) could partition the network. Over time, more IXPs were built globally. For blockchains, ensuring there are seed nodes and well-connected peers on every continent helps new nodes sync and propagate blocks reliably.

Which frameworks map well: Telecom has metrics like the number of independent routes between points, mean time to recovery, etc. A relevant one is **"K-survivability"** – the network remains connected despite any K-1 node/cable failures. This maps to decentralization: we want a blockchain to remain operational despite loss of some fraction of nodes in a region (K might correspond to how many regions or hubs can fail). For example, if a blockchain can continue if any single country's nodes drop (but not if two specific countries drop), that's akin to 1-survivable at country level. Ethereum's "liveness coefficient" metric ¹⁶ echoes this, stating how many regions' loss would stop finality.

Limits of mapping: Telecom networks are centrally planned to some degree and can be redundantly wired by design. Blockchains rely on participants to set up nodes, so you cannot as easily mandate redundant geography. Also, physical telecom deals with tangible links; blockchains deal with node consensus that has more nuance (a region failing might not physically cut connectivity if there are other nodes elsewhere, but it reduces voting power, etc.). Yet, conceptualizing blockchains in terms of network graphs and applying reliability math is valuable. For instance, one could model the validator network as a graph with nodes weighted by stake and edges by connectivity, then borrow telecom reliability formulas.

Internet Topology and Routing

Internet topology research (often by CAIDA and academic groups) investigates how the internet is structured – AS graphs, router-level maps, etc. A key realization in that field: the internet, though decentralized, has highly central points (e.g., Tier-1 ISPs, major exchange points). Only a few Tier-1 carriers carry a huge portion of traffic, and a handful of submarine cables carry most intercontinental data. For example, a large fraction of Eurasia-to-US traffic goes through one of a few cables under the Atlantic. Similarly, major cloud and content providers (Google, Facebook) carry internal traffic on their private networks that, if disrupted, affect large user bases.

Mapping to Web3: We already discussed AS/BGP analysis in Section 2. If a large portion of blockchain nodes are within a few ASes, that's akin to the internet's concentration: e.g., if 30% of Ethereum nodes are in AWS's AS and another 20% in Hetzner's AS, the AS graph of Ethereum has hubs. The concept of **network centrality** (betweenness, etc.) can identify such hubs. If one AS (say a big ISP) decided to block or throttle blockchain traffic, how many nodes would lose connectivity? There have been instances (like certain ISPs inadvertently or intentionally blocking Bitcoin ports or P2P traffic). Internet researchers use tools like **BGP hijacks** simulation – similarly, one can ask what if a certain country's telecom authority did a BGP hijack to isolate nodes? (This is not far-fetched; it's a known censorship technique.)

Internet topology also teaches about the importance of IXPs. Many networks interconnect at IXPs in cities like Frankfurt, Amsterdam, Ashburn (VA). If blockchain nodes concentrate in those, a problem at an IXP could slow things. Conversely, putting nodes in less common hubs might reduce correlation (though at expense of latency). Topology research encourages mapping where traffic flows. For blockchain, one could map where block propagation flows: e.g., do blocks from a miner in China always go first to a few peers in Europe and then US? If so, those links are critical. Solutions might involve diversifying peer selection deliberately across geographies (like each node ensuring some peers in other continents).

The internet's **robustness comes from redundancy and adaptive routing**; blockchains have redundancy in nodes but currently static routing (each node has a set peer list). Perhaps blockchains could incorporate more adaptive peer discovery when they detect partitions (e.g., if European nodes suddenly can't reach US nodes, they might try connecting via Asia or alternative links). Such ideas mirror internet routing failover.

Which frameworks map well: Graph analysis of centrality, **Herfindahl index** of AS usage (as done by some studies), and **multi-layer network** modeling (treating the overlay and the physical network as layers) all map well. In fact, blockchain networks can be studied as an overlay on the physical internet; any robust design should consider the physical layer. Concepts like **Small-world networks** (the internet has a small diameter due to hubs; blockchain P2P networks often randomize connections but might still have short path lengths) are relevant to propagation efficiency vs risk of hub dependence. Also, measuring **latency distribution** between nodes is akin to measuring internet distance distribution – important to see if all nodes are in a tight cluster (low latency among them) vs widely separated (some links high latency).

Limits: One difference is that internet routing cares about optimizing paths, whereas blockchains care about consensus – not exactly the same. But delays in message delivery (due to topology) can be detrimental to consensus speed and fairness. Another difference: the internet can reroute around damaged links almost automatically (if BGP finds a new path), whereas blockchain nodes can't easily find new peers in seconds – that process is slower, which could lead to minutes of partition. So blockchains might need more proactive measures to emulate the internet's adaptability, perhaps by having backup peers or satellite links (as Blockstream does for Bitcoin).

Content Delivery Networks (CDNs) and IXPs

CDNs like Cloudflare or Akamai distribute content to edge servers globally to reduce latency. They effectively *centralize infrastructure but distribute presence*. They also create points where a lot of content passes (which could be vulnerable if those points fail). IXPs (Internet Exchange Points) are physical facilities where networks meet to exchange traffic locally instead of long-hauling it. Both CDN and IXP concepts highlight *geographical placement for optimal performance*.

Mapping to Web3: One challenge in Web3 is *latency vs decentralization*: if you spread nodes out widely, average latency for data (like block propagation) increases. CDNs show a model where data is replicated in many places to be close to end-users. In blockchain, every full node replicates the whole chain – in a sense, blockchains already CDN their data (every node has a full copy). But because of consensus, it's not just serving static content, it's interactive. Still, the idea of *edge nodes* might be relevant: maybe light clients or caching nodes in various regions could speed things up without requiring every validator to be near every user.

IXPs hint at something: maybe blockchain nodes could purposely cluster at some network hubs to improve inter-node bandwidth, but that conflicts with decentralization – or does it? If multiple independent nodes operate at an IXP (like multiple companies each have a server in an IXP data center), they are separate entities but physically close, so blocks propagate fast among them. That's good for efficiency but if that IXP goes down (power outage at that facility), many nodes drop at once – correlated failure. It's a trade-off that maps exactly to the decentralization question. Ethereum's high concentration along the Atlantic might be partly because Frankfurt and Virginia (Ashburn) are huge IXPs making it efficient ⁹⁶ ⁹⁷. So the protocols might inadvertently encourage clustering where internet infrastructure is best (which is exactly in those hub regions). This is analogous to CDNs placing servers at IXPs.

Which frameworks map: CDN performance metrics (latency to users, cache hit rates) aren't directly relevant, but the overall strategy of replicating widely to improve resilience is. More relevant is **disaster scenarios** considered by CDNs – e.g., how to serve content if one region is offline (maybe route users to next nearest cache). For a blockchain, how to maintain consensus if a region (with many validators) is offline? Possibly pause block production until they rejoin (like Cosmos chains halting, which is safe but not livened), or continue with reduced quorum (some protocols allow that at security cost). It's akin to CDN degraded mode.

IXPs also give an idea of cooperative infrastructure: different entities sharing a hub for mutual benefit. In blockchain context, maybe nodes can share certain infrastructure (like a common relay network such as BloXroute for block propagation in trading) to speed things up. But that introduces centralization risk if that shared relay fails or censors. Indeed, Ethereum's MEV-Boost relay is like a CDN for blocks – a handful of relays (Flashbots, BloXroute, etc.) distribute blocks quickly to validators. It improved performance (faster block propagation) but at cost of centralizing block distribution (only a few relays were used, raising censorship risk ⁹⁸ ⁶⁸). The community identified that risk and has been trying to decentralize the relay layer or at least have many relays (which they have increased). This parallels how having multiple CDNs avoids reliance on one.

Limits: CDN infrastructure is centrally managed; blockchains can't fully mimic that as they operate peer-to-peer. But the concept of layer-0 (physical) and layer-1 (P2P overlay) interplay is instructive: blockchains might incorporate more explicit topology awareness (maybe nodes forming locality clusters but ensuring some long-distance connections too – basically implementing a structured overlay like Kademlia which ensures certain distance properties).

Energy Grid Redundancy and Power Supply

Electric power grids are often cited for needing decentralization to avoid blackouts. Concepts include **not putting all generators in one area**, having **grid interties** so regions can support each other if one fails, and maintaining **spinning reserve** (excess capacity in case a plant goes offline). Also, grid operators worry about **cascading failures** – one station fails, overloads others, causing chain reaction (like the 2003 Northeast blackout in the US).

Mapping to Web3: The idea of excess capacity or redundancy maps to ensuring more nodes than needed (which blockchains do have – you only need some fraction honest; more nodes give safety margin). Cascading failure is analogous to, say, if one big mining pool stops, others might get overloaded with mempool backlog or if one country's nodes drop, maybe it leads to lower block production and then maybe others get slashed or penalized inadvertently, compounding issues.

National grids have **islanding** concepts – if the grid splits, each part tries to operate on its own to avoid total collapse. In blockchains, if a network partition happens (islanding the network into two groups), consensus typically fails (or forks) unless one part has $>2/3$ (in PoS) and can continue alone. That's akin to one grid island having enough generation to meet its demand. Designing blockchains to handle partitions gracefully (maybe halting and later reconciling) is tough, but perhaps insights from grid re-synchronization (when two grid islands reconnect, careful phase alignment is needed – similarly, blockchain forks need reconciliation) could apply.

Which frameworks map: N-1 reliability in grids (the grid can lose any one generator or line and still supply demand) is similar to the idea that the blockchain can lose any one validator or even a set of them and still finalize blocks. We often speak of f fault tolerance – e.g., tolerant to losing up to 33%. That's akin to N-1 if one third of validators constitute one “critical component”. We might extend grid thinking: they consider N-2 events sometimes (two failures at once). For blockchain, tolerance often stops at the threshold ($>33\%$ offline stops finality in Ethereum). Could we design to tolerate more? Not without trade-offs (like reduced security). But maybe by having *auxiliary power* – in grids, if main plants fail, emergency generators kick in. In blockchain, if many validators go offline, could light clients or backups pick up temporarily? Perhaps a radical idea: an emergency consensus mode with lower quorum if many are offline (with security trade-off). That's analogous to brownout procedures in grids (maintain minimal service in crisis).

A specific adjacency: the Texas winter storm 2021 – too many generators in one region (wind in West Texas) froze, causing grid collapse. A parallel: if too many Ethereum validators are in one state (say all in a certain data center that loses power due to weather), the network can lose finality temporarily (this actually happened on Ethereum in May 2023 for other reasons – finality was lost for an hour due to a bug and many validators failing to attest simultaneously, not geographic but demonstrates risk of correlated failure). The lesson is to have *diverse energy sources or weather zones*. Blockchain analogy: diverse jurisdictions/climates so one event (storm, heatwave causing data center cooling failure) doesn't catch majority of nodes.

Interestingly, Bitcoin mining has begun to emphasize geographic diversity partly for energy reasons – miners chasing cheap power globally (hydro in one place, flare gas in another, solar elsewhere). This diversifies geography naturally. However, that can still concentrate regionally (e.g., too many in one state's grid can still be cut off by that grid's failure).

Limits: The power grid is a controlled system (operators can shed load to stabilize, etc.), whereas blockchains are decentralized with no central controller to stabilize if things go awry (except perhaps core devs coordinating an emergency hard fork – rare and slow). So resilience has to be built-in, not managed in real-time easily.

Supply Chain Concentration Metrics

Supply chains (for anything from microchips to medical supplies) have metrics for concentration risk. For example, a **Herfindahl-Hirschman Index (HHI)** is used to quantify supplier concentration (an HHI near 1 means one supplier dominates, near 0 means very fragmented). Also metrics like **time-to-recovery** for if one supplier fails, and **geographical diversification** of suppliers (companies track how

many suppliers in each country, to avoid all in one hazard zone). COVID-19 showcased how concentrated supply chains (e.g., most PPE from one country) is risky.

Mapping to Web3: We can treat each component of a blockchain's operation as a "supplier" of security or resources. For instance, miners are suppliers of hash power; stake validators supply security and validation service. If too much of that supply comes from one entity or region, risk is high. Indeed, measures like **Nakamoto coefficient** are essentially akin to saying "how many suppliers (validators) do we have to compromise 33% of stake?" – similar to asking "if the top 3 suppliers of component X go down, can we still produce our product?" The **geographical Nakamoto coefficient** proposed (liveness coefficient ¹⁶) is like the number of region-suppliers of security needed.

We could also adapt HHI: The Ethereum paper defines *geographical HHI* for stake ⁹⁹ – if all stake in one region, HHI =1, if evenly spread, HHI lower ¹⁷. This directly borrows from economics. They also use *geographical Gini* ¹⁷ which is another measure of inequality among regions. These are exactly supply concentration metrics applied.

Another supply chain concept is **"single source vs multi-source"**: e.g., do we rely on one cloud provider (single source for hosting) or multiple? Multi-sourcing is recommended to reduce risk, albeit at cost of complexity. For blockchains, multi-sourcing of infrastructure means ensuring nodes are on multiple providers. The earlier stat about "neither AWS nor Hetzner individually is over one-third" ¹⁰ is an example of demonstrating multi-sourcing (two big providers, neither dominant alone).

Systemic risk in supply chains often uses simulation of node removal: what if supplier A is lost? In blockchain, we can simulate removal of all nodes in X region – does the network continue? The result might be binary (stops finality or not). You could map that to an **impact score**. For instance, losing all US-based validators might drop Ethereum's participation to ~70% (since ~30% are US ⁶⁹), which is below the 66.6% needed for finality (so finality stops). That's a critical risk. Losing all German nodes (~15%) still leaves ~85% so finality continues fine. This suggests "USA is a critical supplier" in Ethereum's supply chain of consensus – something similar to a manufacturing chain where if one big plant goes offline, production halts vs if a smaller one goes offline you manage. So applying those what-if analyses from supply chain risk management can quantify and identify critical geographies.

Limits: Supply chains can relatively easily diversify by adding more suppliers in new regions (though with cost). Blockchains can't directly "add more independent validators in Africa" by decree; they can only create incentives and hope operators emerge. Also, blockchains don't have the notion of inventory or stockpiling – you can't stockpile block production. When it stops, it stops immediately. So resilience has to be constant, not something you can compensate for later (except you could maybe "make up for lost blocks" but that's not how consensus works normally).

Systemic Risk Modeling (Finance)

In finance, systemic risk refers to how the failure of one entity (like a big bank) can cascade through the system. Tools like stress tests, network contagion models, and metrics like **"too big to fail"** identification are used. There are also analogies in portfolio theory: don't put all assets in one region or sector to avoid correlated losses.

Mapping to Web3: If we consider each jurisdiction or infrastructure provider as a node in a risk network, systemic risk modeling might examine: if jurisdiction X cracks down, what fraction of the network is affected and does that cause a collapse of trust or service? For example, the OFAC sanction on Tornado Cash in 2022 caused >60% of blocks to be censored ⁷⁰, arguably a systemic shock to

Ethereum's ideal of neutrality. The network didn't stop, but it compromised a property (censorship-resistance), which is analogous to a financial system remaining operational but credit not flowing to certain areas – a partial systemic failure.

Financial risk models often consider **correlations** – how likely many components fail together. For blockchains, geographic correlation is key: nodes in one country are likely to fail together under certain events (legal or internet outage). So one could assign correlation coefficients to validators based on country or AS. For example, two validators both on AWS us-east are highly correlated in failure; two, one on AWS us-east and one on a home server in Brazil, are less correlated. Then one could calculate an overall risk of >33% failing as a probability given distributions – akin to how finance calculates default correlation and risk of simultaneous defaults (like credit default correlation in a CDO). This could yield a probability of network failure due to geography – something like: if each region has X% chance of outage per year, what's chance that enough regions fail to break the network? This approach *explicitly uses frameworks from systemic risk*.

Another concept: **stress testing** – imagine extreme scenarios (US bans staking, EU power grid failure, a giant solar flare knocks out certain latitudes' power/internet, etc.) and see if the network could cope (maybe halting is the best it can do, which might be acceptable if it recovers without losing funds). By doing scenario analysis, as done in disaster planning, you can identify vulnerabilities.

Limits: Financial networks have central banks and regulators who can intervene in crises (like bailouts). Blockchain networks aim to be autonomous with no central authority. So if a systemic event happens, there's no built-in rescue mechanism. The analog might be a user-activated soft fork or emergency hard fork – a social-layer intervention to freeze or salvage the chain in face of meltdown (like if >50% fell under hostile control, remaining honest might coordinate a fork). This is akin to central bank intervention albeit chaotic. So systemic risk analysis might show potential collapse conditions but blockchains can't mitigate in real-time, only preemptively by better decentralization or reactively by community decision.

Disaster Recovery Planning

Organizations plan for disasters by ensuring backups, alternate sites, clear protocols when primary systems go down. For example, banks have secondary data centers in another region; companies run drills for earthquakes or cyberattacks.

Mapping to Web3: A fully decentralized network doesn't have an "alternate site" – every node has the full ledger, so in theory any node can be an alternate if others fail. That's good – backups are inherently everywhere (like every full node is a backup of the ledger). But there isn't a concept of "switching control to backup consensus" because consensus is collective. However, one could incorporate disaster recovery by: - Having **fallback communication channels** (if internet is disrupted, perhaps use radio, satellites – Bitcoin does via satellite broadcast, some research into using high-frequency radio for block propagation). - Establishing procedures for when large fractions of nodes drop: e.g., should remaining nodes automatically slow block production or increase timeouts? Ethereum's client updates after May 2023 incident included tweaks to handle lost finality better (basically, nodes will still attest and finalize later once enough come back, rather than grinding to total halt). - Documenting a community response plan: if a region is cut off, do we encourage miners/validators elsewhere to temporarily pick up slack (they naturally will, but maybe ensure no slashing for those cut off, etc.)? For example, some PoS chains might consider pausing slashing if a known disaster (so that validators that go down due to no fault aren't penalized too harshly).

Disaster scenarios like “**what if an EMP hits a region**” or “what if an undersea cable break partitions East/West hemispheres for a day” could be role-played. How would Bitcoin or Ethereum respond? Likely a chain split or downtime. Perhaps improvements could be made (maybe implementing checkpointing or manual reconciliation after partition – which exists in some enterprise blockchains, but not public ones, since it violates trust assumptions).

Which frameworks map: Business impact analysis (BIA) from DR planning – identify critical processes (for blockchain: block production, transaction inclusion) and what resources (nodes, network) they require, then see what happens if those are unavailable. We already have metrics like time-to-finality, which in disasters could become infinite if finality halts. We might want to define RTO/RPO (Recovery Time Objective / Recovery Point Objective) equivalents: how quickly do we want the network to recover finality after X% nodes go offline? And how much data (blocks) might we lose or need to re-org (like a Recovery Point – ideally zero blocks lost, which is why halting might be safer than continuing on partial partitions).

Some blockchains explicitly think in these terms: e.g., **EOSIO chains** had features to pause when less than some percent of block producers remain – a kind of built-in DR strategy to stop and wait rather than proceed insecurely.

Limits: Traditional DR assumes a central authority can reboot systems elsewhere; decentralized networks rely on the protocol rules and participants. So the biggest “plan” might be ensuring the protocol itself is robust enough to handle as many scenarios as possible automatically (like tolerate up to 33% down). Beyond that, it’s human coordination. The resilience that is there (all nodes having data, etc.) is good but not complete if consensus fails.

Insights that map well: The notion of **geographic risk zones** – DR planners often keep backups far from the main site (e.g., not both in same flood plain). By analogy, ensuring node replicas in different risk zones (different countries, climates, legal regimes). That’s exactly geographic decentralization. Maybe in future, protocols could encourage risk-zoning: for example, at network launch, deliberately recruit validators on different continents rather than all from one. Some permissioned chains did this – e.g. Libra (Diem) originally wanted validator association members from different countries to avoid one regulator jurisdiction.

Identifying Frameworks That Map Well vs Not:

- **Map well:** Redundancy and failover concepts (telecom, grids, DR) – blockchains need redundant nodes and paths. Metrics like HHI, Gini, Nakamoto coefficient – directly used already ¹⁷ ⁹⁹ . Risk analysis methods (scenario simulation, stress tests) – could be applied to blockchains to quantify risk of centralization.
- **Map well:** Multi-factor definitions of decentralization (like in management science: political, economic, etc. as in the Open Knowledge reference ¹⁰⁰) – blockchains also have facets: governance decentralization vs technical vs geographic – similar to how governance decentralization in government has administrative, fiscal, political (though that reference is about governments ¹⁰¹).
- **Map partially:** The internet’s adaptive routing – blockchains don’t have this by default; trying to incorporate it could conflict with consensus rules (e.g. dynamically changing peer topology might cause unpredictable propagation times). But some adaptability is possible (like adjusting timeouts, or nodes seeking new peers if old ones vanish).

- **Map partially:** Financial bailout mechanisms – blockchains have no central bank, but the “community hard fork” is a last-resort analog. That is slow and painful (like Ethereum’s DAO fork or potential forks under pressure, e.g., if OFAC compliance became too high, some mooted a user-activated soft fork to slash censoring validators – a drastic community action akin to regulatory intervention).
- **Not strongly applicable:** Some public sector decentralization measures (like the **Regional Authority Index** in government ¹⁰² that measure political power distribution) don’t translate because blockchains don’t have sub-governments (though one might analogize miners in each country as “power centers”). But blockchains aren’t hierarchical as governments are, so those specific indices are less useful.
- **Not directly applicable:** Traditional *corporate DR plans* assume controlled environments. Blockchains can’t plan in the same way with assigned roles. They rely on protocol pre-planning.

In conclusion, interdisciplinary insights confirm many intuitive points: a decentralized system should avoid single points of failure (telecom, power grids), diversify critical components (supply chain, portfolio theory), and be prepared for correlated stresses (systemic risk, DR). Where decentralized networks differ is the lack of centralized coordination during crises – which means the design and incentive structure must bake in resilience from the start. Geography is a major factor in all these analogies: whether it’s not having all power plants in one region or not relying on one country’s undersea cable, spreading out is key to withstanding shocks. The following sections will leverage these insights to compare formal frameworks and address structural risks and solutions more directly.

5. Comparing Frameworks and Taxonomies for Decentralization

Over the years, various organizations – academics, industry consortia, standards bodies, and think tanks – have attempted to formalize what “decentralization” means and how to measure it. Here we review some prominent frameworks and taxonomies, focusing on what they include, what they miss, points of consensus, and points of divergence. We also examine specifically how (or if) each treats geography in their definition.

Vitalik’s Trichotomy (Architectural, Political, Logical Decentralization)

One oft-cited informal framework comes from Vitalik Buterin’s 2017 blog post defining decentralization in three dimensions: **architectural (decentralization in the number of physical computers)**, **political (decentralization in control/governance)**, and **logical (decentralization in the software interfaces or data structures)**. In that view: - *Architectural decentralization* roughly corresponds to distribution of nodes – which has a geographic aspect (how many physical machines, and implicitly where). - *Political decentralization* means no single or small group controlling – that touches geography if, say, all decision-makers are in one country (then politically maybe a single jurisdiction influences them). - *Logical decentralization* means the system doesn’t have a singular point of failure in its data model (blockchain is logically one ledger but can be considered logically centralized in that sense, interestingly).

Vitalik’s framework was more conceptual, cautioning that people often conflate these axes. It’s consensus in the community that decentralization is multifaceted; his breakdown became a common reference. However, it wasn’t a metric system, more a taxonomy to discuss trade-offs. For instance, a system could be architecturally decentralized (many nodes) but politically centralized (nodes controlled by one entity).

Geography treatment: Vitalik didn’t explicitly list geography, but it fits under *architectural decentralization* – a system spread over many nodes across the world is more architecturally

decentralized than one confined to a server cluster. Also *political decentralization* could indirectly cover geography: if all powerful actors live under one government, politically the system is vulnerable.

Vitalik's viewpoint is largely complementary to later frameworks, not contradicting them. It sets the stage that no single metric will capture decentralization – there are at least these axes.

Are We Decentralized Yet? / Nakamoto Coefficient

Balaji Srinivasan and Leland Lee introduced the **Nakamoto coefficient** around 2017 as a simple measure: the minimum number of entities needed to control $\geq 51\%$ (or one threshold) of a given subsystem (mining, stake, etc.) ¹⁵. They proposed measuring multiple subsystems: e.g., mining power, client software (how many client implementations to reach $>50\%$ usage), exchange custody (how many exchanges hold $>50\%$ of coins), etc., to gauge different centralization aspects.

The website “Are We Decentralized Yet?” built on this concept, listing major blockchains and metrics like number of miners controlling 80% hash, number of code repositories or core devs, number of companies controlling $>50\%$ of nodes, etc. It was a rough early attempt.

What it measures: The Nakamoto coefficient gives a single integer per dimension. For instance, if 4 mining pools have $>51\%$ of hash collectively, Nakamoto coefficient for mining is 4. It's easy to interpret (higher = more decentralized). It highlights weak points – e.g., if a chain's Nakamoto coefficient for validators is 2, that's very concentrated.

What it misses: It's a coarse metric. It doesn't differentiate between, say, 4 equal pools vs 1 big + 3 smaller that just cross threshold. It also doesn't consider distribution beyond the threshold – e.g., 51% vs 95% control scenarios get treated similarly if same number of players. Also, it's static – doesn't account for dynamic ability to collude or location. It's an entity-centric measure, not explicitly geographic.

It can be gamed: one entity could split into multiple named entities to raise the coefficient without real decentralization change.

Consensus vs Divergence: There's general consensus that the Nakamoto coefficient is a useful *starting point* or slogan, but insufficient alone. It's now often cited in combination with other measures. Some later frameworks integrated it or refined it (e.g., Messari 2023 said initial Nakamoto coefficient is good but needs updating for PoS context ¹⁵).

Geography treatment: The original Nakamoto coefficient by Balaji didn't explicitly handle geography. However, people have applied the concept to geography: e.g., “country-level Nakamoto coefficient” – how many countries would need to collude to control $>50\%$ of hash or stake. That's basically the liveness or censorship coefficients we discussed ¹⁶. The Yang et al. 2025 paper indeed defines a “liveness coefficient” which is essentially the Nakamoto coefficient applied to regional distribution (they sort regions by stake and find smallest set over 33% stake for liveness risk) ¹⁰³ ¹⁰⁴. So academic frameworks have extended it to geography. In industry, we also see mention of “X countries account for $>50\%$ ” which implies a geographic Nakamoto number (like 2 countries for Ethereum ~ US+Germany $> 50\%$ of nodes possibly).

The ConsenSys Research Approach (Decentralization Benchmarks)

In 2019, ConsenSys researchers (Everett Muzzy et al.) undertook a study on measuring Ethereum's decentralization over time ¹⁰⁵ ³⁷. They identified 19 subsystems across 4 categories ¹⁰⁶ (like client diversity, mining pool concentration, developer distribution, etc.). Notably, they *omitted geographic and power grid factors* because those were “not on-chain or necessarily quantifiable” at the time ¹⁰⁷ – but they acknowledged their importance. They tracked things quarter-over-quarter, producing data visualizations (like how Gini of supply changed, number of nodes changed, etc.).

What they measure: Their approach was comprehensive: from token distribution (whale holdings) to network nodes to dapp usage, etc., trying to capture decentralization of not just base consensus but ecosystem. It was like creating a multi-dimensional dashboard rather than a single score.

What they miss: As they said, they missed explicitly geography and legal jurisdiction factors ¹⁰⁷. They also couldn't quantify dev power relationships well (they mentioned those might be more qualitative). They also risk Gresham's Law as Walch warned ³⁸ – focusing on what can be counted (like node counts, ETH distribution) and possibly underemphasizing tricky aspects like influence networks.

Consensus vs Divergence: Many agreed with their notion that decentralization must consider many subsystems. However, not everyone wants to track all those – some just focus on the key ones (consensus and governance). Their effort was unique but not repeated regularly in public; it served more as a one-time analysis to say “hey, here's how Ethereum is trending.” It did show consensus in the idea that decentralization is not one thing. Divergence: others might classify differently (e.g., maybe break categories into governance, network, wealth, etc., but they had 4 categories anchored in architecture).

Geography treatment: They explicitly note they consider legal jurisdictions and power grids important but did not quantify them ¹⁰⁷. They even mention “strength & distribution of power grids on which nodes run and the legal jurisdictions and stability of countries in which nodes are hosted” ¹⁰⁷ as omitted factors, showing they thought about geography but found it hard to measure at that time. So their framework flagged it as a known blind spot – which is a win for transparency.

Their reluctance to include it (due to lack of data) contrasts with Messari 2023 where by then tools existed to measure node distribution, so newer frameworks do include geography.

Academic Frameworks and Indices

Academically, besides Nakamoto coefficient mentions, frameworks include: - **Decentralization in Bitcoin and Ethereum networks (Gencer et al. 2018):** They measured multiple metrics: distribution of mining power, distribution of nodes by IP, connectivity of network (they found Bitcoin's P2P was more decentralized in connectivity than Ethereum's at the time) ⁶⁵ ¹⁰⁸. They didn't propose a single index, but concluded that by various metrics, both had some centralization (pools in Bitcoin, etc.). They advocated measuring at multiple granularities (e.g. top-10 vs top-50 miners controlling X%). - **Tuwiner's Decentralization Index (hypothetical):** Some independent bloggers tried to create indices combining factors (like 0-100 score weighing nodes, distribution, etc.). Not widely adopted because weighting is arbitrary. - **EU's work on Crypto asset decentralization:** Recently regulators think about how to measure if something is sufficiently decentralized. They might consider things like how many entities control consensus, how public is participation, etc. Not formalized yet but divergent definitions likely (some might say if any identifiable governance group exists, it's not fully decentralized, regardless of node count).

Consensus: Academically, consensus exists that there is no single scalar metric that captures decentralization well ³⁸. Most papers measure a set of metrics (Gini, Nakamoto, entropy, etc.) and present them collectively. Many use similar metrics: concentration ratios (like top-4 control X%), entropy, Nakamoto coefficient.

Divergence: They diverge in which metrics they prioritize. E.g., one might argue *network connectivity decentralization* (peer degree distribution, etc.) is crucial, another focuses on *ownership distribution* (like distribution of stake or wealth). Some frameworks, like one by Bezawada et al. (just hypothetical example), might incorporate user-level decentralization (how many clients are run by how many users – very hard to know).

There's also divergence in how to interpret metrics. For example, one standard body (say ISO) might come up with thresholds: "decentralized if no single entity has >X% control." Others say decentralization is a spectrum not a binary. Walch's critique suggests we not oversimplify to binary, a view many share.

Industry/Standards Formalizations

No ISO or NIST standard for "decentralization degree" exists yet as far as I know (NIST has reports on blockchain tech but not a metric standard). However: - **Crypto Rating Council (CRC)** had a methodology to judge if an asset is a security; one factor is decentralization of development and issuance. It wasn't quant heavy and more binary (e.g., is there an identifiable promoter? If yes, more likely security). - **BIS (Bank of International Settlements)** in some reports measured how concentrated mining or validation is, because of financial stability concerns. - **MiCA (EU regulation)** indirectly touches on decentralization (like if an entity offers a stablecoin, how centralized is governance – requiring whitepapers to disclose governance structure). - **IEEE or W3C:** There might have been groups (like IEEE Blockchain) discussing taxonomy. Possibly Vitalik's categories are referenced. The W3C's Decentralized Identifiers (DIDs) spec actually had criteria for what makes a DID method decentralized vs centralized, which includes whether the ledger it uses is decentralized and if there's a single authority. That's quite relevant: they required DID methods to ideally use permissionless networks or at least not have a single point of failure. It's not numeric but principle-based in standard.

Geography in standards: So far, not explicit. They focus on control distribution and technology, but not on node geography. Possibly in future, regulators might require disclosing if >X% of validators in one jurisdiction, because that implies jurisdictional influence. But at present, no numeric threshold standard.

Consensus vs Divergence Summary

Consensus Points: - Decentralization is multi-dimensional. A single metric like "number of nodes" is universally seen as insufficient ³⁷. - Power distribution matters more than raw counts (Phil Daian's statement ²⁶ resonates with others; hence metrics often revolve around control of resources, e.g., stake or hash). - Many use similar tools: Gini coefficient for inequality of something (stake, hash), HHI for concentration ¹⁷ ⁹⁹, share of top K entities, Nakamoto coefficient variants – so there's a common statistical toolkit. - Transparency about metrics is valued. Walch's critique ³⁸ is often cited, implying frameworks should be careful not to oversimplify. ConsenSys research explicitly noted assumptions and omissions ⁶⁷.

Divergent Points: - **What dimensions to include:** Some frameworks consider **development decentralization** (how many independent dev teams, etc.), others ignore it. E.g., Ethereum is open-source but if a few teams maintain it, is that centralized? Vitalik's viewpoint would call that political maybe, but some metrics skip it. - **Scope of network:** Some focus only on consensus (miners/

validators), others include user interfaces (if everyone uses Infura or Metamask, is that a centralization? Some argue yes: Ethereum might have many nodes but if most users rely on one RPC provider, there's a central point in practice). - **Thresholds vs continuous:** Some want a binary label: is it decentralized enough (e.g., security law context). Others say it's always a spectrum and context-specific. - **Geography divergence:** Many early frameworks neglected it explicitly, focusing on control by entity rather than location. Newer work (Flashbots, Messari) emphasize geography as important ¹⁸ ¹³. So there's a shift to include it. Some might still argue geography is secondary – e.g., if 5 independent US validators control a network, some might say it's decentralized enough politically (5 parties) even though geographically one country, while others say that's not good enough because one government can target all 5. So frameworks diverge if they care about jurisdiction diversity as a first-class requirement. - **Quantification approach:** Entropy-based indices vs simple counts vs fancy agent-based modeling (like Yang et al. simulate equilibrium centralization rather than just measure static). Academics often bring advanced metrics (like that *geographical payoff coefficient of variation* ¹⁰⁹ ¹¹⁰ measuring fairness disparities). Industry frameworks usually keep it simpler.

How geography is treated (or not): - Frameworks in 2018 or earlier (Gencer, Vitalik's, ConsenSys 2019) largely did not explicitly measure geography, though they acknowledged it qualitatively. - By 2023, frameworks (Messari, Flashbots, Yang et al.) explicitly incorporate geography metrics ¹³ ⁵. There's emerging consensus *now* that it's a key dimension to measure. - Divergence remains in how to weigh it: Is 30% nodes in one country acceptable? There's no consensus threshold. Some say as long as <50% in one place, it's fine (no single jurisdiction majority), others may desire much less.

In summary, earlier taxonomies gave us conceptual clarity (e.g. Vitalik's axes) and basic measures (Nakamoto coefficient). Later ones attempt holistic or specialized metrics (ConsenSys's multi-metric, Flashbots simulation's novel metrics). No single framework has been universally adopted as "the decentralization index", but a combination of measures is standard practice. There is growing convergence that any serious analysis should include at least: distribution of power (stake/hash), distribution of nodes (often by geography or infrastructure), and possibly distribution of influence in governance. Where definitions diverge is often on subtle points like how to measure influence or how to treat user-level centralization (exchanges, custodians controlling lots of funds is a kind of centralization not of the protocol but of the ecosystem).

The lesson is that decentralization is context-specific: Bitcoin's priorities might weigh miner distribution more, Ethereum's might weigh validator client diversity and MEV issues, etc. But any taxonomy that completely ignores geography is increasingly seen as incomplete ¹⁸ ⁵, given events like China's mining ban and US sanctions that demonstrated geographic clustering leads to real effects ¹ ¹¹.

6. Structural Risks of Geographic Concentration

Geographic concentration in a supposedly decentralized network can create multiple **structural risks** – situations where the network's security, availability, or neutrality is undermined due to nodes being clustered under the same external conditions or authorities. We will detail how such concentration impacts various critical properties, using both conceptual reasoning and real-world or modeled scenarios.

Censorship Resistance Erosion

Risk: If a large portion of validators/miners reside in one country or jurisdiction, that government can enforce censorship on the network's transactions. Decentralized networks prize being permissionless and censorship-resistant – anyone can transact and the network will include it. But if, say, 60% of block

producers are in Country X, and Country X's law says "do not include transactions from sanctioned address Y," those producers will comply or face penalties. This leads to a de facto censorship on a supposedly global network.

Evidence: This isn't just theoretical: - After the U.S. Treasury's OFAC sanctioned Tornado Cash addresses in 2022, Ethereum saw many U.S.-based validators (especially those using MEV-Boost relays like Flashbots) start omitting those transactions ⁷⁰ ⁷¹. Within weeks, over 50% and peaking near ~80% of Ethereum blocks were OFAC-compliant (i.e., censoring) ⁷⁰. Essentially, because a majority of stake (through Lido, exchanges, etc.) was under U.S. influence, they followed U.S. regulations, resulting in censorship at the protocol level. This clearly shows how geographic/regulatory concentration translates to censorship: Ethereum's nominal protocol didn't enforce censorship, but the validators' locale did. - While the community responded (by encouraging non-censoring relays, etc., which brought it down to ~27% by mid-2023 ⁷²), the incident demonstrated the fragility. Publicly, this was a huge controversy; Ethereum's claim to neutrality was tested. Many argued Ethereum was "under attack" by regulation ¹¹¹, or at least at risk of splitting into a censored vs uncensored fork if things worsened.

- In Bitcoin, direct on-chain censorship hasn't visibly occurred widely, but mining pool concentration by country has raised concerns. Under China's dominance (pre-2021), the Chinese government could have conceivably ordered pools to censor certain transactions (they didn't, beyond their normal rules), or after 2021, U.S.-based pools could face similar pressure. In 2021, Marathon Digital, a U.S.-based miner, announced they mined an "OFAC-compliant block" (censoring certain txs) as a demonstration. The backlash was strong and they reverted that policy soon after. But it signaled that as mining moves under U.S. jurisdiction, the temptation or expectation to censor "illicit" transactions could rise.

Implication: If censorship becomes systematic, the network effectively loses a key value proposition. Users from certain regions or associated with certain activities could be excluded from using "global" networks. It also introduces a **partition risk**: some validators/miners might refuse to censor (especially if in other jurisdictions), leading to potential chain splits where one part of the network includes a transaction and another rejects it. That's basically a fork along geopolitical lines, undermining a single unified chain.

Corollary: It might only take one dominant jurisdiction to flip a network's policy. So a network heavily concentrated in a single jurisdiction is one regime change or policy away from losing neutrality. If tomorrow Country X bans all non-KYC transactions from being processed, a network where most validators are in X either halts (if they stop processing lots of tx) or becomes a filtered network. Truly decentralized networks want that to be impossible or at least very difficult (requiring global coordination among many governments, which is much less likely).

Correlated Infrastructure Failures and Outages

Risk: Geographic concentration often means infrastructure concentration: many nodes using the same power grid, ISP, data center region, etc. Thus a single event – a power outage, earthquake, fire, network outage – can knock out all those nodes simultaneously. Blockchains generally assume failures are random and uncorrelated, so that the probability of a majority failing is astronomically low. Correlated failures break that assumption, presenting a scenario where a big chunk (potentially >33% or >50%) of nodes drop at once, which can halt or compromise the network.

Evidence and Scenarios: - Power Outages/Natural Disasters: If most miners of a cryptocurrency are in one country, a large-scale power outage (like the one that hit Texas in Feb 2021 or South Africa's load-shedding) could take them offline. For Bitcoin, there was a smaller example: In early 2021, Xinjiang

(China) experienced an outage for safety inspections which reportedly caused Bitcoin's global hash rate to dip ~20% overnight, as many mining farms in that region went dark. The network continued (20% less hash just slows blocks a bit until difficulty adjusts), but if that had been larger (say 50%), block times would slow drastically until adjustment, affecting usability and possibly causing price and network uncertainty. - For proof-of-stake, a >33% outage means loss of finality: Ethereum experienced this in May 2023 due to a technical bug – finality stopped for ~25 minutes as many validators stopped attesting, then resumed ¹¹². That wasn't geographic, but if, say, Europe's internet went down (maybe from a massive cyberattack or misconfigured BGP route – things that have happened regionally), and if European validators >33%, Ethereum would similarly not finalize blocks until they recovered. If >50% were offline, the chain might not even produce blocks (depending on protocol rules). - **Cloud/ISP Outages:** We saw how an AWS outage in us-east-1 region in 2025 impacted many crypto services and nodes ¹¹³ ¹¹⁴. Specifically, it was reported ~37% of Ethereum EL nodes went offline and L2 networks like Base had reduced capacity ¹¹⁴ ²⁰. The Ethereum network didn't fail completely because 63% were elsewhere, but performance and ancillary services degraded. If AWS had an even larger share or if multiple clouds coincidentally had issues (e.g. a major internet backbone cut affecting all providers in a region), more than 50% nodes could drop. In such a case, Ethereum's consensus might stop finalizing or even producing. Non-final blocks might continue for a while (the honest minority tries to keep going) but finality wouldn't resume until enough came back or the chain reorganizes to new majority. - **National Internet Blackouts:** Several countries have had government-implemented internet shutdowns (e.g., during protests or crises, like Syria, Iran, etc.). If such a blackout occurred in a country hosting many nodes, those nodes would be cut off. Example scenario: Imagine 40% of a network's validators are in Country Y and Country Y shuts down external internet for a week – those validators can't communicate with the rest, effectively offline. The network now runs on the remaining 60%. If 60% \geq supermajority threshold, the network can still finalize blocks but the 40% are seen as offline and might be slashed for not participating (if PoS). If 60% < threshold, the network might halt finality or halt entirely (if consensus requires a fixed validator set majority). So correlated failure leads to at best degraded operation, at worst total halt. - Even if the network continues with the remaining, when Country Y comes back online, their nodes might find they're far behind or slashed for downtime. This is a recoverable situation (they'd sync up), but it's messy. Worse, if that 40% continued producing blocks amongst themselves (partitioned network), you now have a fork – resolving that can be ugly (like chain re-orgs or manual reconciliation).

Correlated failures thus threaten availability and consistency. They turn an assumption of independent failures (which underpins safety margins like “with 33% honest online, it's fine”) on its head by creating effectively a single giant failure event.

Legal/Regulatory Intersection: A “failure” can also be legal: e.g., if one jurisdiction seizes mining farms or orders staking nodes offline. That's a correlated node failure triggered by law enforcement rather than physical outage. The China mining ban was such a case: overnight, ~50% of hash went dark as miners shut down ⁸. Bitcoin survived via difficulty adjustment after two weeks, but that period had slower blocks. It was a planned correlated shutdown. Another example: If a major exchange-run staking operation (say Coinbase Cloud) decided or was forced to shut down all its validators (maybe due to regulation or business decision), a large chunk of stake would vanish at once. The network would adapt if under threshold, but it could cause a shock (slashing events, etc., if not gracefully handled).

Network Topology Collapses: Another angle: if nodes cluster in one AS or physical location, a single misconfiguration could isolate them. For instance, in June 2019, a Cloudflare outage briefly took down a lot of internet services. If many blockchain nodes rely on Cloudflare's DNS or CDN in some way, that could hamper them connecting. Or a BGP hijack by a malicious actor could isolate or split a cluster of nodes (imagine an attacker hijacks the IP ranges of half the Ethereum validators; those validators can't

communicate outside and form a subnetwork – possibly leading to two networks that can't see each other, causing consensus failure or a fork).

Summary: Geographic concentration creates a “common mode failure” risk. Blockchains are robust against random node failures but not so much against common mode failures. The impact includes: - Temporary or prolonged halting of block finality or production. - Potential chain splits if partitioned. - Penalties for validators (slash for downtime) which further weaken the network because previously bonded stake is now penalized, possibly reducing security or creating contentious hardfork debates to restore funds (if event was beyond operators' control). - Loss of user confidence: if the chain halts for hours/days due to a regional issue, it undermines the idea of global 24/7 operation. E.g., would you trust a payment system that stopped finalizing for a day because one country had an outage?

Flashbots researcher Quintus noted “if a protocol requires more bandwidth or lower latency than a region offers, that region will not see participation” ¹¹⁵ – the reverse is also true: if many participants depend on a region's infrastructure, when that infrastructure falters, the protocol suffers.

Thus, correlated infrastructure failures are a prime argument for geo-diversity: the network should be able to “heal” or continue if any single region or provider fails – the N-1 criterion analog. If we can't achieve that, then the system has a hidden central point.

Jurisdictional and Legal Risks

Risk: When nodes concentrate in one or a few legal jurisdictions, the network becomes subject to those jurisdictions' laws and regulations, potentially compromising its autonomy. Governments can enact laws or issue court orders affecting nodes: forcing them to censor (as above), to surveil, to confiscate keys, or even to shut down. If enough of the network is under one government's thumb, that government could **co-opt or cripple the network** without any technical attack, simply through legal pressure.

Examples & Discussion: - **OFAC Sanctions & Compliance:** Already covered in censorship, but beyond censorship, legal risk includes regulators potentially deeming the network illegal or requiring licenses to run nodes. For instance, if the U.S. or EU decided running an unregistered crypto node is unlawful (far-fetched perhaps, but imagine under AML concerns), nodes in those countries (which might be majority) would shut down or go underground. - **Legal Orders to Fork or Freeze:** If most miners are in one country, a court could order miners to refuse blocks from a certain address or even to attempt a fork to freeze certain funds (akin to how courts order freezing bank accounts). Decentralized networks resist this because usually not all will comply, but if all are under one court's jurisdiction, they might have to. - **Intellectual Property or Other Laws:** Jurisdiction can impose, say, export controls. A fun hypothetical: if many nodes are in the U.S., and someone stores illegal content (like copyrighted data or worse, contraband) in a blockchain transaction, U.S. law might demand nodes not propagate that. This happened in minor ways: e.g., some blockchain networks have illicit content encoded; it's theoretical that hosting that data violates law in some countries. If a majority of nodes follow one country's law on this, they might collectively purge or refuse blocks with such content, effectively altering protocol behavior. - **Tax or Economic Measures:** A government could slap heavy taxes or energy tariffs on mining, making it economically unfeasible, thus pushing miners out or forcing consolidation to fewer subsidized players (which could be state-influenced). E.g., during high energy crises, some countries told miners to shut off to save power. If one country with many nodes does this, it's a de facto partial network shutdown event (like Kazakhstan in early 2022 curbing mining due to blackouts, which caused a hash rate dip). - **Nationalization or Co-option:** In extreme cases, a state might attempt to nationalize mining facilities or coerce staking pools. If, say, 50% of a network's stake is held by entities in one country, that government could demand those entities use their stake to vote in certain ways or include

backdoors. If they refuse, they face punishment, if they comply, network is compromised. - **Legal Systemic Risk:** If one country legally defines major aspects (like classification of the tokens as securities or commodities), it can indirectly centralize control – e.g., if all validators in that country must be licensed companies, then effectively the government gatekeeps who can validate, centralizing entry.

We saw a mini-version with the Tornado Cash sanction: not only censorship, but it raised questions: could U.S. regulators push Ethereum towards compliance blockchain where certain transactions are not allowed at protocol-level? The fear was if >66% validators would only build on censoring blocks, eventually non-censoring validators would be forced off the canonical chain or slashed (if considered attacking). That fortunately didn't fully materialize (non-censoring relays persisted and share fell to ~27% OFAC-compliant blocks ⁷², meaning many started including all tx again), but had it grown, Ethereum might have faced a fork: one chain following OFAC, one ignoring – a geopolitical schism in the network.

Another subtle risk: If a network is dominated by one country and that country decides the network is a strategic asset or threat, it could either co-opt it (like treat it as critical infrastructure under state supervision) or shut it down domestically. For example, if hypothetical "Country A Coin" (which is global, but heavily mined in Country A) becomes too important, Country A's government might pass laws to influence it, as a matter of national policy. This alters the power dynamic of "no one controls it" to "one government has outsized influence".

Correlated Legal Moves: The worst-case scenario is multiple major jurisdictions coordinating (e.g., US + EU both impose similar restrictions on blockchains). If 80% of nodes are in US/EU combined, a joint policy could effectively become network policy. It would no longer be permissionless global network but subject to Western rules. This is not far-fetched – already FATF Travel Rule is being globally applied to exchanges. One could imagine future international standards requiring "Responsible blockchain operation" meaning known validators etc. Decentralization can thwart this if nodes are sufficiently in other places, but concentration invites it.

Loss of Credibility/Community Splits: Aside from direct effects, if a blockchain becomes obviously controlled by one jurisdiction's rules, users from other parts of the world may abandon it or create alternatives. It undermines the universal trust. For instance, after OFAC incident, there were talks of spinning off an "Ethereum uncensored" chain if it got worse. That fragmentation is harmful to network value and is itself a systemic risk.

In summary, heavy jurisdictional concentration effectively means the network's fate may be decided by a single legal regime rather than by code or global consensus. That runs against the ethos of being above any one nation's whims.

Overreliance on Cloud and Hosting Providers

Risk: We touched on physical outages, but there's also a **business risk:** If a few hosting providers (like AWS, Hetzner) host a majority of nodes, those companies have the power to affect the network. They could decide to kick blockchain nodes off (due to policy or contract changes), or suffer outages as already discussed, or possibly be compelled by governments (as AWS has contracts with US Gov, it could be pressured to help enforce something on its servers).

Evidence: Hetzner in 2022 explicitly banned crypto mining and node operations on its infrastructure (they said running Ethereum nodes violated their ToS, ironically as Ethereum moved to PoS and likely lots of nodes on Hetzner) ¹⁰. This created a scramble: many nodes were using Hetzner, especially for

Ethereum and Solana. If Hetzner had actually mass-removed them (they didn't immediately, but it was a looming threat), it could have knocked a large fraction offline. As of mid-2022, Hetzner was hosting ~16% of Ethereum nodes (by one measure) and an even bigger chunk of Solana validators. If they pulled the plug all at once, that's a correlated failure. It's legal/contractual rather than physical, but similar effect. Node operators would have to migrate—likely causing downtime, maybe some slashing for offline PoS validators during the move.

AWS hasn't banned crypto at large, but AWS has terms that could conceivably be interpreted to restrict illicit activity etc., and they have in the past removed specific customers (e.g., Parler social network was deplatformed by AWS in 2021). If running a node becomes seen as risky or undesirable, AWS could unilaterally cut service to many at once. Even without malicious intent, the convenience of cloud means many might accidentally configure similarly or depend on AWS services like NTP, resulting in correlated behavior (like if AWS NTP had a glitch and all AWS-hosted nodes got wrong time, they might behave strangely in consensus simultaneously).

National-scale outages (revisited): Many cloud providers have zones in certain regions (AWS us-east-1 is infamous because a lot relies on it). A serious event like a hurricane or cyberattack causing a cloud's regional failure is not impossible. Already happened in smaller scale (the DynamoDB DNS issue causing multi-region cascade in 2025 ¹¹³ ¹¹⁴). Overreliance basically reduces the network's redundancy: it's like having all backups in the same building.

Cloud reliance also has a censorship component: Even if not government-driven, a cloud provider might decide to block certain blockchain traffic (perhaps to manage bandwidth or to appease regulators preemptively). If so many nodes sit behind a few cloud IP ranges, if those ranges are traffic-shaped or firewalled, big parts of network get partitioned or slowed.

Nationalization of Clouds: If tensions rise, cloud infrastructure might be targeted by state actors (cyber warfare, etc.). If nodes were more peer-to-peer on residential lines, they might be more distributed and less juicy targets than huge data centers that can be hit to affect thousands of nodes.

Operational Capacity in Crises: We combine this bullet with one mentioned: if in a major crisis (pandemic, war), having all nodes in one area could mean not enough people can maintain them if that area is hard hit (like during COVID in 2020, some data centers had to plan for staff being sick). A global spread ensures that even if one country's operators are incapacitated, others elsewhere keep things running.

Example: War in Ukraine 2022 – some Ukrainian and Russian miners had to shut down or relocate. Bitcoin hash dropped a bit when war started (though overshadowed by larger moves). If a conflict happened in a region with many validators (imagine a Taiwan conflict affecting East Asia's internet/power where some crypto operations are), those nodes might vanish or be taken over.

National-scale Internet filters: Some countries (China, Iran) have national firewalls that block or throttle certain traffic (like Tor, certain protocols). If a majority of nodes are in open internet now but in future more networks fragment, a country could throttle P2P traffic which might cause nodes inside that country to only talk internally (partition from global network or at least slower connectivity).

Operational note: Many node operators rely on services like Infura/Alchemy for sending transactions or monitoring. If cloud reliance is high even for users, an outage can make the network *seem* down even if consensus is working (e.g., Infura outage in 2020 prevented many Ethereum wallets from functioning, even though chain was fine). That's another type of central point (infrastructure-level) that isn't about

validators but the ecosystem. In decentralization context, reliance on a few infrastructure providers like Infura is often criticized as “web3’s weak point”. This doesn’t compromise consensus, but it does impact effective decentralization (if everyone’s using one API, that API can censor or fail). That’s adjacent but relevant.

National or Regional Outages and Partitioning

We covered this largely under correlated failures, but to specifically mention national-scale outages: - **Natural disasters:** e.g., a huge earthquake in California knocks out power and internet for a large region hosting many nodes (maybe Silicon Valley companies). That’s sudden drop of those nodes. - **Geomagnetic storm:** a rare but possible solar storm could knock out power grids or satellite comms in a hemisphere. That could disable a majority of nodes if they’re all on affected power grids. (This is extreme, but the point of structural risk is thinking worst-case). - **Government-ordered kill switch:** Some authoritarian regimes can shut down internet nationally (like Egypt did in 2011). If we imagine an even more extreme scenario where a major country with lots of nodes (US, for anti-cyberattack reasons or something) temporarily cuts external connectivity (perhaps unrealistic, but not impossible in war context), the network splits or halts.

Each such scenario results in either a chain halt (if threshold unreachable) or chain split (if two groups operate separately, potentially both thinking they are majority if time goes on). The recovery from either is painful: - In a halt, what if the outage lasts long? In PoS, prolonged downtime can lead to things like needing manual interventions or chain restarts in some designs. In PoW, network resumes when miners come back but difficulty might be off, etc. - In a split, rejoining the network means one side’s blocks get orphaned which could include many transactions (some might be important like exchange deposits – confusion and double-spend risk arises if two partitions processed transactions independently).

Operational Capacity in Crises

This was the last bullet: consider if in a crisis event, can the network’s operators continue to function and respond? If all core devs and node operators were in one country undergoing crisis, updates or mitigations could lag. For example, if a critical security bug is found, normally devs worldwide coordinate a fix. If most are in one region that’s knocked out by disaster or war, who will deploy the fix or even communicate it? A globally distributed dev and node community is more robust – someone awake and with power/internet can take charge if others cannot.

One might recall during COVID how different regions of the world were affected at different times; global operations shifted loads around. If node operations were similarly global, a local outbreak wouldn’t drop the network.

Summary of Structural Impacts:

- **Censorship Resistance:** Erodes with geo concentration (network can become effectively permissioned by dominant jurisdiction) ¹¹ ¹² .
- **Fault Tolerance to Outages:** Severely reduced; network no longer tolerates large-scale correlated outages, leading to halts or forks (as seen in mining ban, AWS outage scenarios) ¹⁹ ⁸ .
- **Legal/Regulatory Capturability:** High – one or few governments can co-opt the network’s rules or shut it down, undermining sovereignty of the network.
- **Recovery Complexity:** Partition or correlated failure requires complex recovery – possibly manual – undermining the “always on, automated” claim of blockchains.

- **Trust and Credibility:** If events repeatedly show the network bending to one country's will or going down because one provider had issues, users will lose trust in its resilience and neutrality. It becomes no better than centralized systems in perception.
- **Economic Impact:** A chain halt or fork can cause chaos in markets (prices crashing, derivatives liquidations, etc.). E.g., if Ethereum stopped finalizing for a day, DeFi protocols might pause or misbehave, causing ripple financial effects. So structural risk is also systemic risk to the crypto financial ecosystem.

By analyzing these structural risks, it becomes clear why geographic decentralization is not a mere idealistic goal but a practical necessity for robustness ¹ ¹¹⁶. Networks must aim to avoid these single points of failure – whether they be physical, political, or infrastructural – to truly achieve the resiliency and censorship-resistance that justify their existence.

7. Gaps and Challenges in the Field

Having surveyed existing knowledge, it's evident that understanding and measuring geographic decentralization still faces significant gaps. These gaps span data availability, methodological weaknesses, and conceptual blind spots where current approaches break down. We identify key areas where information is missing or approaches fail, and highlight needs for new techniques.

Incomplete and Biased Data

One fundamental gap is simply **knowing where nodes are** with confidence. Despite all the methods discussed, our maps of node locations are still **partial and probabilistic**:

- **Unreachable Nodes:** Many nodes do not appear in crawling results because they're behind NAT or firewalls (especially home users, who arguably contribute to decentralization). For example, ProbeLab explicitly notes their data excludes nodes behind NAT ²³, which could be a sizable unseen portion. Ethernodes or Bitnodes might only see a few thousand reachable peers, while the actual node count (including hidden ones) might be higher. Thus, geographic breakdowns often ignore a potentially more distributed set of nodes that are not publicly reachable. It's possible that those hidden nodes are more geographically diverse (since many might be hobbyist nodes around the world), meaning our measurements might *overstate* centralization because we see mostly the data center nodes. Or conversely, maybe hidden nodes cluster similarly. The gap is: we don't know.
- **Geolocation Accuracy:** IP databases can be wrong, especially for less common regions. Developing countries often have IP ranges that map to ISP HQ address (which might be in the capital, even if user is elsewhere). So data might show more nodes in capitals or big cities than reality. Some countries (like small states) share IP allocation with others. There's anecdotal evidence of nodes geolocated to incorrect countries due to IP quirks. Without ground truth (operators self-reporting), verifying this is hard.
- **Dynamic Node Populations:** Node distribution is not static; nodes come and go daily. Our measurements are often snapshots. If one looked at different times, especially if there are events (e.g., after China ban, nodes relocated), the distribution changes. We lack continuous historical data for many networks. For Bitcoin nodes, we have periodic snapshots, but not a smooth timeline beyond big events. For Ethereum, Cambridge CCAF started providing time series around Merge, but it's still early. This means we can't easily see trends like "is decentralization improving or worsening over years" except in coarse ways (like we know Bitcoin mining went from China-heavy to more distributed, but exact progression month by month is rough).
- **Who is a Unique Operator:** We don't always know if multiple nodes in different places belong to one entity (like one miner with farms in two countries, or one staker running nodes on multiple clouds). Operator-level centralization might be higher than geographic if one entity spans regions (which is a hidden centralization, albeit a mitigating factor for geographic risk if one entity deliberately diversifies locations). Our data might treat them as independent nodes, overstating decentralization. This is a privacy challenge – mapping entity identities is non-trivial and often only approximate via addresses or known pool names.
- **Metrics on Non-**

blockchain P2P networks: If we consider "decentralized networks beyond blockchains" (the user suggested considering beyond blockchains in design), data gaps are even larger. For instance, how geographically distributed is the Bittorrent DHT or Tor relays? There are studies, but not continuous. For blockchains, at least some groups track things; for decentralized storage like IPFS, far less is known. So designing an "index" or methodology applicable across decentralized networks is stymied by widely varying data availability.

Methodological Breakdowns and Assumptions

Even with data, our methodologies often **rely on assumptions that can break:**

- **Assuming Honest Responses for Triangulation:** Methods like BFT-PoLoc assume an honest majority of probes or some honest nodes to anchor trust ⁶⁰. If an attacker controlling many nodes tries to fool triangulation by adding delays, results skew. Also, if the network itself is under adversarial conditions (like someone running Sybil nodes to confuse measurements), our inference techniques might map Sybils and think they're distinct.
- **Sybils and Counting Nodes:** A big challenge in decentralization metrics: do we measure nodes, or entities? Many networks can be Sybil-attacked (one entity runs many nodes). If an entity spreads its nodes across geography, one might think "oh, there are nodes in 5 continents, looks good," but if they all obey one master, not actually good. Most of our measuring techniques can't easily tell apart independent vs Sybil nodes. Some approaches try (like Heimbach 2025 using network fingerprints to cluster validators under one operator ⁴⁶). But a gap remains: fully anonymous networks can be dominated by Sybils that appear in data as separate. E.g., counting Bitcoin nodes – someone could run hundreds of nodes on cloud across zones to appear worldwide, boosting apparent decentralization. It's expensive to do at scale for long, but possible. So any count or geo distribution could be gamed.
- **False Precision and Misleading Aggregates:** We repeatedly mention risk of false precision ⁴. Many current studies still report precise percentages without error bars. The gap is formalizing uncertainty. Researchers seldom publish confidence intervals for "X% nodes in country Y." But ideally they should: e.g., "we scanned N nodes, confidence that between 25-35% in US." Not doing so can mislead non-experts to over-trust numbers. It's partly a communication gap: how to convey uncertainty easily. We need methodologies that incorporate uncertainty quantification.
- **Attribution of Effects:** If we observe centralization outcomes (like censorship level or performance issues), pinpointing exactly how much is due to geography vs other factors is tricky. For example, if block propagation is slow, is it because of distance or because of a few nodes throttling traffic? Or if a censorship event happened, was it entirely because nodes in US complied or also because maybe some non-US chose to comply voluntarily to follow majority? Multi-causal situations are hard to attribute. Our frameworks are mostly descriptive, not causal. We lack models to say "if distribution was more even, censorship level would drop to X%." We can simulate (like Yang et al. did differing distributions ³¹), but those are as good as model assumptions.
- **Narrow Focus of Metrics:** Each metric often measures one dimension, but focusing on one can mask others. E.g., a network might have good geographic spread but poor client diversity (all nodes run same software – a bug could take all down). If our decentralization index weighted geography heavily, it might score high while ignoring that single client risk. Industry frameworks attempt multi-factor scoring, but there's no agreed weighting. New metrics like "Cost of Kidnapping" mentioned in Flashbots salon ¹¹⁷ try to improve on Nakamoto by considering cost to compromise nodes. But those require difficult estimation (cost in what terms? Bribery, coercion?).
- **Methodologies for content vs consensus:** For networks like Filecoin, measuring decentralization includes content replica distribution. That's a different domain (you need to verify file locations, which is why proofs like GeoPoRet are proposed ⁶¹). Traditional blockchain metrics don't cover that. The gap is custom methodologies for specific network purposes (storage, bandwidth, compute networks).
- **No Standardization:** A significant gap is the lack of standard definitions and methods accepted broadly. Each research or report reinvents or uses slightly different measures. This leads to confusion or non-comparable results. For example, one study might say "40% of nodes in US" meaning of reachable nodes as of one date; another says "30%" including all (with an estimate for behind NAT). There's no

standard dataset or approach, making it difficult to track progress or consensus. In a sense, the field lacks a "benchmark dataset" or "reference scenario" to calibrate methods. One attempt is the CCAF index providing a consistent method at least for Ethereum, but it's still new and not transparent (they provide an interactive map but not raw data to third parties easily, I think). - **Determining Optimal or Adequate Decentralization:** Methodologies break in determining success criteria. We can measure decentralization, but what's good enough? Should no country have >20% of nodes? Should Nakamoto geo coefficient be at least 5? There's a gap in linking metrics to outcomes: e.g., if censorship probability is our outcome, what distribution yields negligible censorship risk? That connection is not clearly quantified in guidelines. Without target thresholds, it's hard to say where we stand or when to declare something dangerously centralized.

Blind Spots and Unmeasured Factors

Even a comprehensive approach might **miss some factors**:

- **Social Layer Centralization:** Perhaps the biggest intangible: a network could have globally distributed nodes, but if development and governance are centralized (e.g., one core dev team dictates changes, one foundation holds huge influence), then effectively control is centralized. Case: Binance Smart Chain had many validators globally, but it was alleged that most are coordinated by or known to Binance (so political centralization). Our geographic measures would say "looks decentralized across many countries," missing the control aspect. We touched on this in frameworks: it's hard to quantify but critical. Angela Walch often points out miners/validators are not the only locus of power – devs and key stakeholders have power too. Our current measures hardly account for this, except indirectly maybe by number of clients or diversity of dev teams.
- **Economic Centralization:** Ownership of coins or wealth concentration can lead to centralization of influence (like big holders could bribe or control validators). It's partly measured by token distribution Gini, etc., but not directly geographic unless wealth is regionally concentrated. That's a gap: no one ties token distribution by geography often. Could be interesting, e.g., if 80% of a coin's supply is held by addresses believed to be in one country, that country has influence via law on those holders. This is rarely measured due to privacy (we can guess exchanges and maybe region of usage but not precise).
- **User-level decentralization:** A network might have many nodes but if users all connect through a handful (like nearly all light wallet users connect to Infura or Etherscan's node), then effective central points exist. This aspect – how decentralized is access – is not captured by node distribution alone. It's a gap because a censor could just hit those public gateways and affect most users.
- **New Tech Effects:** Emerging trends could change things – e.g., use of **privacy tools** like Tor by nodes. More Ethereum nodes use Tor now, making geolocation harder (which is good for their privacy but gives us less insight on distribution). If a big portion goes dark in measurement because they hide, then our measured decentralization might falsely look lower (we might not count Tor nodes as in any country, or might clump them as "in Tor network"). Right now Tor usage isn't extremely high, but if it grows, methodology must adjust. It's a gap in forward-looking approach.
- **Interdependencies:** Some decentralization measures assume different aspects are independent, but they might correlate. E.g., a country with cheap energy might have lots of mining *and* that might correlate with certain ISPs, etc. This means a single event (like country ban) triggers multiple issues (loss of mining and maybe dev community if they're there). We often measure each separately but not the combined risk. There's a gap in integrated risk assessment.
- **Data on Minor/All Networks:** We have relatively more data on Bitcoin, Ethereum. But what about the thousands of altcoins or new networks? Many might be *more* centralized, but we have scant data to quantify. If someone wanted a "decentralization index across all networks," data for many is lacking beyond maybe number of validators. For enterprise or permissioned chains, geography often trivial (run in one country), but in analyzing the whole ecosystem, data sparsity is a gap.

Needs for New Techniques

Given these gaps: - **Better Node Discovery:** Tools to find behind-NAT nodes (maybe via peers reporting them, or incentivizing voluntary pingback from hidden nodes) to get fuller pictures. - **Metadata sharing:** Possibly encourage node operators to optionally share anonymized location data (like country flags) into the network for research, with privacy preserving methods (maybe aggregated by clients). - **Continuous Monitoring Infrastructure:** Like ProbeLab but extended, to track multiple networks consistently over time, making data open for analysis. Right now it's piecemeal per team. - **Improved Geolocation Approaches:** Combining methods (as we plan in Section 8) to reduce error. Also, incorporating user-provided ground truth to calibrate (maybe run some known nodes and see how often geolocation gets them right). - **Sybil-resistant metrics:** Possibly weight nodes by some measure of stake or longevity to mitigate dummy nodes. Or focus on validator identities which are harder to fake in PoS (since stake is needed). - **Linking to Outcomes:** Develop models linking decentralization metrics to probabilities of bad outcomes (censorship, outage). This would help answer "how decentralized is enough?" If model says "with >3 independent regions none >33%, chance of complete finality loss <1% per year under assumptions," that could guide thresholds. - **Community & Governance Info:** There's a gap in quantifying decentralization of governance (like how many independent dev teams, how proposals are decided, etc.). Possibly incorporate things like number of entities with commit access to code, distribution of node software usage (client diversity — which Ethereum monitors and we have stats for, e.g., no client >70% ideally). - **Frontier networks:** We need new measurement techniques for networks that use different structures (e.g., partially connected graphs, sharded networks where validators are split into committees by geography maybe). For instance, if a sharded chain tries to assign nodes to shards randomly, measuring each shard's geo distribution might be needed because a shard might accidentally cluster nodes regionally at one time.

In short, current methodologies give a decent snapshot of where things stand but could be missing a large part of the iceberg underwater. Being aware of these gaps is crucial – as our stance of methodological transparency dictates – so that we don't overclaim certainty. It also points researchers where to focus: closing these data and method gaps will significantly improve the fidelity of decentralization assessments.

In summary, the field needs: - more **data coverage** (including historically and across networks), - more **robust inference techniques** (to handle adversaries and uncertainties), - **integrated multi-dimensional analysis** (covering technical, economic, governance facets), - and ultimately a **clearer picture** of how decentralization correlates with outcomes, so we know what gaps are most urgent to fill.

8. Proposing a Hybrid Measurement Methodology

Given the strengths and weaknesses of various approaches outlined, we propose a **hybrid methodology** to measure geographic decentralization (and decentralization more broadly) that synthesizes the strongest elements of existing methods. The goal is to produce a more reliable, transparent, and comprehensive assessment. This methodology will incorporate multiple data sources (modalities), assign weights in a clear way, include reproducible steps, provide uncertainty estimates, and explicitly state assumptions and limitations.

Multiple Inference Modalities in Parallel

No single technique is sufficient; thus, our approach collects and analyzes data from **several modalities concurrently**: 1. **P2P Network Crawling:** Continuously crawl the network's peer-to-peer layer to discover reachable nodes (e.g., using Ethereum's discv5 or Bitcoin's addr messages). This provides IP addresses, peer connectivity info, client types, etc. For *unreachable nodes* (not directly found), use

indirect discovery through peers (peers often announce other peers). Maintain a database of all node IDs seen over time. 2. **IP Geolocation and Cloud Mapping:** For each IP found: - Query multiple geolocation databases (to cross-verify) for country, city. - Check IP against known cloud/IP ranges (using services like ipinfo, or maintaining an updated list of cloud provider CIDR blocks) ¹¹⁸. Tag node as “AWS us-east-1”, “Hetzner hel1”, “residential ISP X in country Y”, etc., whenever possible. - If an IP is found in one DB but not another (discrepancy), flag it for manual review or mark with higher uncertainty. 3. **Latency Probing:** Deploy lightweight probe servers in various regions (North America, Europe, Asia, etc.). From these, periodically ping known nodes (perhaps using application-level ping if needed to get through). Use this to infer approximate distance or at least to validate gross outliers from IP geolocation. For instance, if IP says “Germany” but ping from Germany is 150ms while ping from Australia is 20ms, something's off – possibly misgeo or a proxy. Use this to correct or widen uncertainty for certain nodes. (We assume cooperation in that nodes respond to ping; if not, skip those). 4. **Node Self-reported Clues:** Encourage node operators to optionally provide metadata (e.g., in Ethereum's ENR there could be a field for location if they opt in) – though expecting many to do so is unrealistic, any that do can serve as ground truth points. Additionally, monitor if any nodes use domain names (sometimes peers are “node.country.project.org” which might hint location). 5. **Operator Attribution:** Use on-chain/staking information to group nodes by operator when possible. For PoS, if two validators use the same withdrawal address or belong to the same staking pool, mark them as one operator group (with multiple location points). For PoW, use mining pool tags from coinbase signatures to see how hash is distributed (e.g., Blockchain.com's pool share chart ¹¹⁹). This isn't pure geographic, but it overlays an operator layer. We then know, for example, pool F2Pool has servers in US and CN – that one operator spans regions. We incorporate this by not over-counting them as independent influences in metrics like Nakamoto coefficient. 6. **Alternate Routes & Resilience Testing:** To gauge network resilience, occasionally simulate node failures in analysis: e.g., remove all nodes in country X from the dataset and see connectivity or consensus threshold remaining. This isn't exactly measurement but analysis, contributing to the interpretation of the data. 7. **Social and Governance Data:** Though harder to quantify, track how many distinct entities (and their countries) are involved in core development and governance (like number of different countries from which protocol improvement proposals come, or where core dev teams are based). This contextual data might not feed into a numeric index directly but is reported qualitatively alongside, because a network run entirely by developers in one country might face similar risks as nodes in one country.

By running all these in parallel, we address different facets: (1) and (2) give baseline distribution and infrastructure usage; (3) validates and refines that; (5) and (7) add context of control and governance beyond raw nodes.

Transparent Weighting and Scoring

For creating an index or summary metrics, our methodology uses **transparent weighting**: - We present raw metrics for each category (node count by country, by AS, stake by country, etc.) individually first, with citations ¹¹⁴ ⁹. Then, if needed, combine them into composite scores with clearly stated formula. - For example, one composite “Geo-Decentralization Score” could be calculated as an average of normalized sub-scores: - Distribution of nodes (e.g., using entropy or HHI of nodes across countries). - Distribution of stake/mining power across countries (weighted by stake rather than just node count). - Distribution across hosting providers (cloud vs non-cloud HHI). - Jurisdictional Nakamoto coefficient (number of jurisdictions to reach 50% stake). - Etc. Each of those can be scaled 0-100 and then averaged (or weighted if we decide some are more critical). The weights must be explicitly chosen and justified – e.g., we might weight stake distribution by country higher than raw node count, because stake = power in PoS. We might weight cloud distribution lower if we think jurisdiction is more important, but that choice must be documented. - We will also produce specific “Nakamoto numbers”: e.g., “It takes 2 countries to control >50% of hash (namely Country A ~35%, Country B ~18% so together ~53%)” ¹²⁰. Or

"N largest hosting providers that host >50% of nodes is N=2 (AWS and Hetzner) ¹⁰." These are easy-to-understand measures we include. - For each metric, we include the data source and any adjustments. E.g., "Using IP geolocation, we estimate 30±5% of nodes in US ¹⁹. After latency verification, no major reclassification was needed." This transparency ensures the weighting is not a black box: the consumer of the report can see the underlying figures and how they were combined.

If we create a single decentralization index, we might do something like:
$$\text{Index} = 0.25 * (100 - \text{HHI}_{\text{country}}) + 0.25 * (\text{Nakamoto coefficient (jurisdiction)} \text{ score}) + 0.25 * (100 - \text{HHI}_{\text{cloud}}) + 0.25 * (\text{client diversity or dev decentralization score})$$
 (This is an example; actual formula to be justified by correlation with risk factors). We will footnote that formula in the report so it's clear.

Reproducible and Open Methodology

To ensure credibility: - **Open Data and Tools:** We would open-source the scraping and analysis scripts (maybe via a GitHub repository). E.g., provide code to perform the Ethereum peer crawl, the IP lookup (with appropriate API keys or reference datasets), and the analysis notebooks that calculate metrics. That way, others can reproduce or audit steps. This echoes what some researchers do (like open-sourcing their measurement tool; ProbeLab methodology is public ^{23 33}). - **Periodic Updates:** The methodology is designed to be run regularly (weekly or monthly) to track changes. Reproducibility over time by us ensures our own comparisons (the same method used consistently so trends are real, not artifact of method change). - **Neutral Infrastructure:** Use multiple vantage points for crawling/probing to avoid one location's biases. Possibly collaborate with volunteers globally to run measurement nodes (like RIPE Atlas style). This also democratizes data collection. - **Documentation:** Every step is documented in a methodological appendix: how nodes are found, how databases were chosen, how weighting was decided, what version of data (e.g., "MaxMind DB version X from Jan 2025 used"). This allows someone else to replicate with maybe a different database if they want to test sensitivity. - **Citation of Sources:** As exemplified in this response, every factual statement or figure in the final output will cite either our raw data or prior studies. For instance, if we say "37% of Ethereum nodes on AWS" we cite CryptoSlate ¹⁹ or Ethernodes data. For our own original measurements, we'd likely provide a reference to an internal figure or dataset appendix.

Uncertainty Bounds and Sensitivity Analysis

Crucially, our hybrid method will include **uncertainty estimates**: - For each percentage or metric, we calculate an uncertainty. For IP geolocation, we might define uncertainty as ±X% of nodes that couldn't be confidently geolocated (like "10% of nodes lacked reliable data, which if all belong to one country could shift numbers by at most Y"). Or use the variance between multiple geolocation DBs as an indicator of location uncertainty. - When combining metrics, propagate uncertainties. If node count distribution has some error margin, reflect that in final index as a range. We might output: "Decentralization index: 73 (range 70–78 considering measurement uncertainties)." - Also do **sensitivity analysis**: e.g., if we weigh factors differently, does the conclusion change? If removing cloud distribution from the index changes ranking a lot, note that. This ensures the index isn't giving false confidence. - Particularly note scenarios: "If all unknown nodes were actually in X country, then share of X could be up to Z%," as a what-if bound.

Including these bounds addresses the false precision risk ⁴. It also guides future improvements (if uncertainty is large, we know where better data is needed).

Explicit Assumptions

Throughout the methodology, list assumptions: - **Network Assumptions:** e.g., "We assume the set of reachable nodes we find represents the distribution of all nodes (with caveat that hidden nodes might differ)." Or "We assume validators not responding in our probe are offline or unwilling, and treat them as if distribution similar to responders." These can be validated if possible (perhaps by comparing with known subsets). - **Geolocation Assumptions:** "Assume IP geolocation at country level is correct for $\geq 90\%$ of IPs, and errors are random (no systematic bias placing nodes in wrong country that would drastically alter top 3 countries counts)." If this assumption might fail (like if an entire ISP is mis-registered in another country), we mention it. - **Cloud identification assumption:** "Assume ipregistry's cloud provider identification is up-to-date. Some small hosting providers might be mislabeled as 'Non-cloud', which could understate cloud share by perhaps a few percent." ¹²¹ - **Stake vs Node assumption:** For PoS, "We assume geographic distribution of stake correlates with distribution of validators we measured (i.e., big validators in region = big stake in region). However, if large stake holders delegate to validators in different locations, our stake-by-country could be off. We attempt to cross-check via known validator operators' locations." - **Adversarial conditions:** "Assume no adversary is actively trying to deceive our measurement (e.g., by running Sybil nodes with misleading IPs or delaying probes). If that assumption breaks, our data could be skewed. We monitor for signs (like multiple nodes with very similar characteristics that might be one actor)."

By laying these out, readers know exactly what trust to place and where caution lies. Also, it sets to-do items: any assumption is a potential target for future method refinement (how to remove or validate it).

Scope and Limits of Claims

Finally, clarify **what this hybrid method can and cannot claim:** - We can claim with data support: distribution of nodes/stake across countries/providers as observed, approximate diversity metrics, etc. We **cannot claim** to pinpoint exact locations or identify every unique operator. For example, we won't claim "Node X is in Berlin at address Y" – that's out of scope and against privacy. We'll claim "likely in Germany" with uncertainty range. - We cannot guarantee we found every node; there may be entire subsets (like an alternative network of Tor-only nodes) that we miss. We'll note such possibilities and perhaps include anecdotal info (like "Approximately 5% of Ethereum nodes are Tor hidden; our method currently counts them but cannot geo-locate them, treating them as 'Unknown'"). - The hybrid method still cannot conclusively link cause and effect (e.g., can't by itself prove decentralization caused some outcome, that is more analysis). It's mainly descriptive but more robust. - Emphasize that **decentralization is multi-dimensional:** this method provides a set of metrics and an index for geographic/infrastructure decentralization, but does not measure everything like dev control or wealth distribution fully. It should be used in conjunction with those considerations for a holistic assessment. - Not a static one-time measure: we note it's meant to be repeated and updated. A one-time score is a snapshot; real decentralization can change with events (like after a mining ban, etc.), so any claims are time-bound ("as of date X, network Y has Z distribution"). - We avoid false certainty: any claim like "Network A is more decentralized than Network B" will be accompanied by specific metric comparisons and possibly noting overlaps in uncertainty if close. We can rank by certain metrics with confidence intervals.

By explicitly stating all this, the methodology remains transparent and honest – a core stance requested ³⁸. It also builds trust such that when the method finds something noteworthy (e.g., "only 2 providers host >50% of nodes" ¹⁰), the audience knows the context and how solid that finding is.

In effect, this hybrid approach tries to marry the *breadth* of industry attempts (cover all relevant factors) with the *rigor* of academic analysis (explicit methods, uncertainties) and the *practicality* of available data

and tooling. It acknowledges uncertainties rather than sweeping them under the rug, which aligns with methodological transparency.

By synthesizing multiple sources, we reduce reliance on any one flawed method and create cross-checks (if IP-based and latency-based inferences agree, confidence is high; if they conflict, we flag that node as uncertain). This multi-modal approach echoes how in other fields (e.g., climate science), multiple models and data sets are combined to get a more robust picture, with error ranges.

The proposed methodology thus represents an evolution from single-track measurements to a resilient framework that can be adopted as a best practice for analyzing decentralization state, informing both researchers and stakeholders of where networks stand and where they might improve.

9. Roadmap for Further Research and Progress

Measuring and improving geographic decentralization is an ongoing process. Here we outline a roadmap of actions, data collection efforts, collaborations, standards, and experiments that would significantly advance the field and help fill the gaps identified.

Enhanced Data Sources and Monitoring Infrastructure

- **Global Node Observatory:** Establish a project (perhaps community-driven like a "Decentralization Observatory") to continuously monitor major blockchain networks using the hybrid methodology. This would involve running distributed crawlers and probe nodes worldwide (similar to RIPE Atlas for internet, but for blockchains). The data (node counts, locations, etc.) would be published openly in real-time or periodic reports. This serves both research and public transparency.
- **Incentivize Data Sharing:** Work with node software developers to include *opt-in telemetry* that helps decentralization research. For example, an Ethereum client could ask "Share anonymous performance and location metrics to help improve the network?" Many software do this for UX improvement. If enough opt in, we get a direct sample of location data (perhaps at coarse level like country or time zone to preserve privacy). Even a sample can validate our inference models (like comparing opt-in self-report vs our IP-based guess for those).
- **Partnership with Cloud and ISP Providers:** Engage cloud providers and major ISPs to potentially share aggregate statistics. For instance, AWS or Google Cloud might (if willing) share what percentage of known blockchain nodes run in each region (they can fingerprint node traffic possibly). Or at least, if we provide IP lists, they could tell us which of those IPs are on their cloud (maybe already done by ipinfo, but direct partnership could ensure up-to-date info even if IP addresses change). Some cloud providers might not want to encourage heavy crypto usage, but framing it as research for network resilience might get more cooperation.
- **Cambridge/Academic Partnerships:** The Cambridge CCAF's work on Ethereum node maps ⁵⁰ is promising. Collaborate with them to extend similar analytics to other networks (Bitcoin, Solana, etc.). Their methodology (open-sourced Armiarma crawler) can be reused for others with adjustments. Academia can provide neutrality and rigor, so supporting grants or projects for them to maintain decentralization indices would help standardize data.
- **Historical Data Backcasting:** Try to reconstruct historical decentralization metrics using whatever archival data exists. For Bitcoin, old Bitnode snapshots, for Ethereum, archive logs from Etherscan or others. This would allow creating time series charts (even if sparse) to show trends (like how Ethereum's distribution changed around the Merge, or how Bitcoin's node distribution changed after certain events). This addresses the user's wish for time series charts if

possible. If direct data lacking, infer from events (e.g., Cambridge mining data can show country share over time for mining; by analogy maybe node count proxies).

Cross-Community Collaboration and Knowledge Sharing

- **Cross-Blockchain Working Group:** Form a working group or forum (perhaps under the Blockchain Governance Initiative Network or similar international bodies) where different blockchain communities share their decentralization monitoring and strategies. For example, Ethereum, Bitcoin, Solana, Cosmos folks could exchange notes on what they've measured and done to improve distribution. This fosters not reinventing wheels and perhaps leads to a unified approach or at least comparable frameworks.
- **Standards or Guidelines Development:** Encourage standards bodies like **IEEE** or **ISO** to consider issuing a **Technical Report or guideline on metrics for blockchain decentralization**. Not necessarily a strict standard yet, but a reference. This could codify definitions (like what constitutes a node for measurement, how to define an independent entity, etc.) and suggest metric calculations. The benefit is consistency and recognition of the importance. The report could draw on our methodology as a reference implementation.
- **Regulators and Researchers Dialogue:** Engage with regulators (e.g., SEC, EU regulators, etc.) who have shown interest in "sufficient decentralization" (for determining securities status, etc.). Share with them these measurement techniques to inform their understanding. Conversely, get insight into what aspects of decentralization they care about (likely distribution of control more than technical node count) – that can shape what metrics to prioritize. This dialogue ensures the research addresses real-world criteria that might be imposed on networks (e.g., maybe a future law says "if >50% nodes in one country, considered not decentralized" – if we know that, we focus on preventing that scenario).
- **Interdisciplinary Research:** Bring in experts from network engineering, complexity science, economics to refine models. For example, collaborate with internet topology experts (like CAIDA) to apply internet mapping techniques to blockchain networks more rigorously. Or with economists to model how incentives drive geographic distribution (like game theory models for miner location choice, as some Flashbots work has done qualitatively ¹²² ¹²³). This can yield deeper insights (e.g., predicting future centralization trends if block reward changes or if latency requirements tighten).

Towards Standards and Benchmarks:

- **Decentralization Index Benchmarking:** Perhaps create a benchmark suite where different networks are scored on decentralization (similar to how there are crypto ratings). If done collaboratively and transparently, it can incentivize networks to improve scores (a bit of competition in decentralization). However, caution that it doesn't become marketing fluff – hence why methodology must be solid. Messari's report is a start by comparing Avalanche, Cardano, NEAR, etc. building on that into a regularly updated "league table" might draw attention to those performing poorly, pressuring them to address issues (like too many nodes on one cloud).
- **Resilience Drills:** Just as disaster recovery in companies, blockchains could run *drills or simulations*: e.g., testnet scenarios where all nodes in a particular region are taken offline to see if network still finalizes (could coordinate with testnet node operators to do a drill). Or simulate latency spikes as if undersea cable broke. Observing testnet behavior can highlight protocol weaknesses which can then be fixed before real occurrences. It also validates whether our risk models (from Section 6) are accurate.
- **Improving Protocol Design:** Feed research results into protocol improvements:
- If latency centralization is an issue (like current Ethereum favors low-latency clustering ⁷ ⁴²), suggest protocol tweaks (maybe longer propagation time, or random delay injection to level playing field) ¹²² ¹²³ .

- If many nodes on cloud, communities can push for grant programs to encourage home/community-run nodes (like incentivize via minor rewards or recognition).
- Cosmos community already tries to diversify validators manually; formalizing such approaches (like recommending new chains to select validators across at least N jurisdictions).
- For existing networks, consider secondary protocols like **proof-of-location schemes** (Ranvir Rana's BFT-PoLoc ⁵⁷) integrated into consensus – that's experimental but maybe one day certain chains will require validators to prove they are not all in one place (like requiring a certain distribution to start the chain).
- **Energy and Location Link:** Encouraging miners/validators to use *renewable energy in varied locations* can hit two goals: environmental and geographic spread (since renewables are widely distributed). Some networks or foundations could subsidize node running in underserved regions (maybe via lower-cost nodes or support). For example, Filecoin launched community miner programs in Africa to get more nodes storing data there (addressing both data distribution and inclusion). These initiatives could be guided by research identifying underrepresented regions where adding nodes would most increase decentralization.

Technical Experiments

- **Alternate Transport Channels:** Experiment with backup communication channels like long-range radio or satellite among volunteer nodes to see if they can keep a network portion alive during internet outages. Blockstream satellite exists for Bitcoin (downlink), maybe explore **satellite uplink or mesh networks** for block propagation as fallback. This isn't mainstream yet but as a research experiment can show feasibility of connectivity even if a country's internet is off.
- **Decentralized RPC networks:** Projects like Pocket Network attempt to decentralize the access layer (RPC). Supporting those and integrating their metrics (like how geographically spread their nodes are) into overall decentralization health is useful. If users can switch to decentralized infrastructure when centralized ones fail, the network as a whole is more resilient. We should research and encourage development of such complementary networks.
- **Probing Attack Surfaces:** It might sound counterintuitive, but conducting controlled *penetration testing* on decentralization: e.g., try to Sybil the network or try to partition it (in test environment or with permission on mainnet) to see how close to the edge it is. This identifies practical vulnerabilities that pure measurement might not reveal. For instance, an attacker might only need to DDoS nodes in 2 data centers to stall a network – a test could simulate that. Finding that out can lead to mitigations (like urging nodes to enable DDoS protection or have fallback peers).

Data Gaps and New Techniques (Recap to drive research)

We specifically aim to address earlier gaps: - *Hidden nodes:* Use techniques like **Network Address Translation traversal** and **peer rumor analysis** to estimate hidden node counts. Or incorporate data from network layer (some ISPs can share how many IPs connect to certain node ports behind NAT via NAT logging – ambitious, but maybe a collaboration with an ISP research group). - *Better geolocation:* Maybe incorporate **WiFi/Geo coordinate** of volunteer nodes to train a model that maps IP latency signatures to location, improving accuracy for those who don't volunteer location explicitly. - *Identify unique operators more robustly:* If possible, combine on-chain identity clues, network clustering techniques, and maybe use machine learning on node behavior patterns (e.g., if two nodes always come online/offline together at same schedule, maybe same operator). - *Macro-level frameworks:* Develop something like a **Decentralization Stress Test** akin to bank stress tests, where given distribution data, we simulate worst-case removal of nodes to see if network passes certain criteria. This could even become a standard: e.g., "Network must pass N-1 country failure (other than the top one) to be considered robust." Researchers and communities can refine what these criteria should be.

Long-term vision: The roadmap ultimately aims for a future where: - Decentralization metrics are as closely watched as price or throughput – making it a key performance indicator of networks. - Users and stakeholders can easily see if a network is trending more centralized and raise alarms. - Networks compete or collaborate to improve decentralization (a healthy dynamic). - Regulators perhaps use objective metrics to differentiate truly decentralized networks from more centralized ones for appropriate treatment (which could motivate projects to decentralize more to meet criteria). - Technically, networks incorporate decentralization-awareness (like Ethereum's research is exploring changes to promote geo-diversity ⁸¹ ¹²⁴, perhaps others will follow).

The roadmap acknowledges that absolute perfect decentralization is unattainable (some factors like global distribution will always have hotspots due to population/economics), but aims for continuous improvement and avoidance of dangerous concentration. It also recognizes that decentralization is not a one-time achievement but an ongoing process needing monitoring and adaptation – hence the emphasis on continuous data, standards, and community efforts.

By following this roadmap, the field will gradually cover current blind spots, reduce the risks identified, and ensure that the promise of decentralized networks (robust, neutral, permissionless) holds true in practice, not just in theory.

10. Maintaining Methodological Transparency

Throughout any analysis of decentralization – and particularly when using the proposed hybrid methodology – it is crucial to maintain a stance of **methodological transparency**. This final section emphasizes how we will communicate our findings and uncertainties, ensuring that for every claim made, we clarify what is firmly grounded in data, what is inferred or estimated, what remains uncertain, and where expert judgment or future input is needed.

Transparency is not just an academic nicety; it's essential for trust. As Angela Walch warned, there's a danger in letting simplistic metrics overshadow nuance ⁴. We aim to combat that by being explicit about confidence levels and assumptions at each step.

Differentiating Grounded Facts, Inferences, and Uncertainties

In our report (and any decentralization assessment): - **Grounded Facts** will be clearly identified and sourced. For example, if we state "As of November 2025, approximately 31% of Ethereum's beacon nodes were in the United States ⁴⁹," that is a grounded fact based on observed data (with a source like ethernodes or probelab weekly report). We will note it as such and provide the reference. Grounded facts are observations with high confidence and consensus – they typically come directly from reliable connected sources or our own measurements with little ambiguity. - **Inferences** will be labeled and explained. For instance, "We infer that a majority of Solana validators are professionally hosted, because over half the nodes have IPs in known data centers ¹⁰." The data (IPs in data centers) is fact, but concluding "professionally hosted" is an inference (likely true, but not directly observed). We'll clarify that it's an interpretation of the data. Similarly, if we say "Geographic clustering likely contributed to the Ethereum censorship issue ¹¹," we base it on correlation (many US validators -> many OFAC-compliant blocks) but it's an analytical inference that if distribution were more global, censorship would have been less. We'll mark that as analysis, not a proven causal fact. - **Uncertainties** and margins of error will be openly stated alongside the numbers. For example: "About 10% ± 3% of Bitcoin nodes are in China as of 2025 – though this is uncertain due to many Chinese nodes using Tor ⁴⁴ (making precise location hard)." Here the "±3%" is an explicit uncertainty range, and the note about Tor indicates why uncertainty exists (unobserved nodes). If we cannot quantify the uncertainty easily, we'll qualitatively describe it

("some nodes could not be located and might slightly alter these percentages if they cluster in one region, but likely not enough to change the overall rankings"). - **Unknowns and Needs for Expert Input:** Where our knowledge or data is lacking, we'll admit it and suggest getting domain expert help. For instance, if we suspect IP geolocation is systematically wrong in Africa (perhaps due to IP assignment quirks), we'll say "We did not find sufficient connected sources detailing node distribution in African networks; consultation with regional network experts or obtaining ISP data would be needed to refine this." This flags to readers that we know this gap and aren't sweeping it away. Another example: "The impact of developer centralization is not captured in our metrics; input from governance experts or further research is required to assess that dimension."

By distinguishing these levels, we ensure readers understand which parts of our analysis are solid and which are tentative or beyond current scope.

Specific Application in the Report

When we present the **executive brief** or main analysis, we'll practice this transparency: - If we make a strong claim like "North America consistently emerges as the focal hub in simulations ⁷⁹," it's because that came from a rigorous study (cited). We'll note that is a model result (with certain assumptions). - When summarizing measurement techniques, we explicitly said what's ALLOWED or not and referenced policy: e.g., "OCR transcription of sensitive PII is allowed" – that was meta-policy from the prompt about image analysis. We won't incorporate that in the final user-facing report, but in doing this analysis, we segregated what we can do (like use those sources) from what we won't (like violate privacy rules). - In Section 6 on structural risks, many statements are scenario-based. We used words like "If", "could", "for example", and provided evidence for each scenario from either real incidents or references. This makes it clear those are not certainties but possibilities informed by past events. - In the proposed methodology, we enumerated assumptions and said we would footnote them in any actual report to users of the index, so they know how results were derived.

Handling of Potential Controversy or Conflicts

It's possible that our analysis might not align with some project's public narrative (e.g., a project might claim to be decentralized, but our data shows heavy clustering). Methodological transparency means if such a conflict arises, we: - Show the evidence (data) for our conclusion. - Acknowledge any counter-arguments or data we lack. For instance, "Project X claims Y, but we observed Z. It's possible our crawler missed some nodes that are not advertised; if Project X provides additional data, we'd incorporate it." This invites dialogue and shows we're not dogmatic. - Stick to objectivity: We don't say "Project X is lying about decentralization," we say "Our independent analysis yields a different result (with specifics) and here's why (methods, data) – the difference could be due to method or undisclosed nodes."

Continual Transparency and Updates

We treat the decentralization assessment as living. If future data or expert feedback shows an error in our method or interpretation, we would update our findings and clearly note the change: - e.g., "Update: After receiving new data from CloudProvider A, we revised the estimate of nodes in region B from 20% to 25%. The earlier report's lower figure was due to mis-classification of some IP ranges as residential which turned out to be cloud B. This correction is reflected in the current numbers." This level of openness about corrections fosters trust that the goal is accuracy, not defending a prior assertion.

In academic style, we might include footnotes or endnotes in the published report detailing minor methodology points or data issues for those interested. But in a user-friendly summary, we'd

incorporate the essence in the text, e.g., "Approximately X% (with a margin of error of a few percentage points)..." or "(data excludes unreachable nodes, which might constitute ~Y% extra, see Appendix for details)."

Why It Matters:

Ultimately, methodological transparency ensures that decisions based on our report (whether by protocol developers, users, or regulators) are informed by reality and not an illusion of precision. It also allows other experts to critique or build on our work, which only improves the field (like Walch's critique improved ConsenSys researchers' care in metrics ³⁸).

By explicitly separating what's **grounded** (e.g., "63% of blocks were OFAC-compliant at peak ⁷⁰ "), what's **inferred** ("implying heavy US influence on Ethereum at that time"), what's **uncertain** ("though it's unclear if some non-compliant blocks were just delayed rather than absent"), and what's **unknown** ("we lack data on how many nodes actively changed behavior due to regulation vs. were offline"), we give a full picture.

This stance also aligns with the ethos of decentralization: **open and verifiable**. Just as blockchain transactions are transparent and verifiable, our claims and metrics should be too, via citations and open methods.

In conclusion, methodological transparency is both a guiding principle of our research process and an explicit section of our report. Every claim will be accompanied by a clarification of its nature: - **Data-backed and certain** (with source), - **Reasonable inference** (with basis and caveat), - **Possible but uncertain** (with explanation of unknowns), - **Beyond current data** (noted as future work or needing expertise).

By doing so, we allow readers to understand the level of confidence and to trust the parts that are solid while appreciating the tentative nature of others. This protects against the misuse of our report (e.g., someone cherry-picking a number without context) because within the report the context is clearly provided.

This practice of transparency is how we ensure our comprehensive deep research not only informs but also educates, enabling others to make well-grounded decisions or further analyses. It is an approach that keeps us, as researchers, honest and the discourse constructive – which is paramount in an area as nuanced and consequential as decentralization.

¹ ⁵ ⁶ ⁷ ⁸ ¹⁸ ⁴² ⁸¹ ⁸⁹ ¹¹² ¹²⁴ [2509.21475] Designing Ethereum's Geographical (De)Centralization Beyond the Atlantic

<https://arxiv.org/html/2509.21475v1>

² ³ ²⁶ ²⁸ ²⁹ ³⁹ ⁴⁰ ⁴¹ ⁴³ Decentralized crypto needs you: to be a geographical decentralization maxi - Research - The Flashbots Collective

<https://collective.flashbots.net/t/decentralized-crypto-needs-you-to-be-a-geographical-decentralization-maxi/1385>

⁴ ²⁷ ³⁷ ³⁸ ⁶⁷ ¹⁰⁵ ¹⁰⁶ ¹⁰⁷ Measuring Blockchain Decentralization | Consensus Research

<https://consensus.io/research/measuring-blockchain-decentralization>

⁹ ¹⁰ ³⁶ ⁹² ⁹³ ⁹⁴ Validator Decentralization: Protecting the Network, Securing the Future

<https://polygon.technology/blog/validator-decentralization-protecting-the-network-securing-the-future>

- 11 12 68 98 **High number of Ethereum blocks censoring US sanctioned users**
<https://protos.com/high-number-of-ethereum-blocks-censoring-us-sanctioned-users/>
- 13 14 15 55 95 **Evaluating Validator Decentralization: Geographic and Infrastructure Distribution in Proof-of-Stake Networks | Messari**
<https://messari.io/report/evaluating-validator-decentralization-geographic-and-infrastructure-distribution-in-proof-of-stake-networks>
- 16 17 31 32 35 44 45 46 53 65 66 78 79 83 84 85 87 88 96 97 99 103 104 108 109 110 116 119 **Designing Ethereum's Geographical (De)Centralization Beyond the Atlantic**
<https://arxiv.org/html/2509.21475v1>
- 19 20 21 22 113 114 **AWS failure exposes crypto's centralized weak point**
<https://cryptoslate.com/aws-failure-exposes-cryptos-centralized-weak-point/>
- 23 24 33 34 54 82 118 121 **Week 2025-39 | ProbeLab Analytics**
<https://probelab.io/ethereum/discv5/2025-39/>
- 25 56 60 86 115 122 123 **Geographic Decentralisation Research Directions - Research - The Flashbots Collective**
<https://collective.flashbots.net/t/geographic-decentralisation-research-directions/5040>
- 30 **Amazon's AWS Failure Shakes Up Crypto's Core Promise - CoinDesk**
<https://www.coindesk.com/news-analysis/2025/10/21/crypto-s-decentralized-illusion-shattered-again-by-another-aws-meltdown>
- 47 69 **Ethereum Statistics 2025: Powerful Facts for Investors - CoinLaw**
<https://coinlaw.io/ethereum-statistics/>
- 48 **Ethereum Node Distribution and Client Usage Revealed - KuCoin**
<https://www.kucoin.com/news/flash/ethereum-node-distribution-and-client-usage-revealed>
- 49 120 **Countries - ethernodes.org - The Ethereum Network & Node Explorer**
<https://ethernodes.org/countries>
- 50 51 52 **Cambridge Blockchain Network Sustainability Index: Ethereum Network Analytics**
https://ccaf.io/cbnsi/ethereum/network_analytics
- 57 64 74 75 76 77 80 117 **Geographic Decentralization Salon @ SBC '25 - Events - The Flashbots Collective**
<https://collective.flashbots.net/t/geographic-decentralization-salon-sbc-25/5143>
- 58 **BFT-PoLoc: A Byzantine Fortified Trigonometric Proof of Location ...**
<https://arxiv.org/abs/2403.13230>
- 59 61 62 90 91 **[2021] File Geolocation via Anchor Timestamping - References - The Flashbots Collective**
<https://collective.flashbots.net/t/2021-file-geolocation-via-anchor-timestamping/2990>
- 63 **BFT-PoLoc: A Byzantine Fortified Trigonometric Proof of Location ...**
<https://arxiv.org/html/2403.13230v2>
- 70 **63% of Ethereum transaction blocks are now OFAC-compliant**
<https://www.theblock.co/post/180158/63-of-ethereum-transaction-blocks-are-now-ofac-compliant>
- 71 **51% of Ethereum Blocks Can Now Be Censored. It's Time for ...**
<https://cryptobriefing.com/51-of-ethereum-blocks-can-now-be-censored-its-time-for-flashbots-to-shut-down/>
- 72 **Ethereum's OFAC-Compliant Blocks Drop to 27%: What Does It Mean?**
<https://dailycoin.com/ethereums-ofac-compliant-blocks-drop-to-27-what-does-it-mean/>

73 This Real-Time Map Shows Why Ethereum's Decentralization Isn't ...

<https://finance.yahoo.com/news/real-time-map-shows-why-080240322.html>

100 Developing Dimensions and Indicators to Measure Decentralization ...

<https://www.mdpi.com/2076-3387/13/11/241>

101 [PDF] Decentralization: Conceptualization and Measurement*

https://projects.mcrit.com/foresightlibrary/attachments/article/1234/Schneider_Decentralization.pdf

102 [PDF] The Difficulty in Measuring Decentralization: The Importance of ...

<https://icepp.gsu.edu/files/2025/01/paper2415.pdf>

111 Ethereum's 'Censorship' Problem Is Getting Worse - CoinDesk

<https://www.coindesk.com/tech/2023/12/06/ethereums-censorship-problem-is-getting-worse>